FATF

盤點資料庫、協作分析及資料保護

2021年7月

FATF（防制洗錢金融行動工作組織）是一個獨立的政府間組織，旨在發展與提升政策，保護全球性金融體系，以對抗洗錢、資恐以及資助大規模毀滅性武器擴散。FATF 建議已成為全球防制洗錢（AML）與打擊資恐（CFT）的公認標準。

如欲進一步瞭解 FATF，請造訪網站：www.fatf-gafi.org

本文件及／或本文所含的任何地域，概不影響任何領土的地位或主權、國際疆界之界定，或任何領土、城市或地區之名稱。

引用文獻：

FATF（2021），*《盤點資料庫、協作分析及資料保護》*，FATF，2021 於法國巴黎，https：//www.fatf-gafi.org/publications/digitaltransformation/documents/data-pooling-collaborative- analytics-data-protection.html

致謝詞

FATF 要感謝公共和私部門的利害關係人 -- 包括技術開發商、金融機構和資料保護機構 -- 為本報告提供寶貴意見、案例研究及回饋。

本報告之工作由 FATF 秘書處（Kristen Alma）領導，並由下述 FATF 代表團之專家小組提供重要建議：加拿大、歐洲委員會、法國、德國、以色列、義大利、日本、評估防制洗錢措施特設專家委員會秘書處、俄羅斯聯邦、新加坡、瑞士、英國、聯合國和美國。

目 錄

縮寫對照表

AI	Artificial intelligence 人工智慧
AML/CFT	Anti-Money Laundering/Countering the Financing of Terrorism 洗錢防制／打擊資恐
API	Application Programming Interface 應用程式介面
CDD	Customer Due Diligence 客戶盡職調查
DL	Deep Learning 深度學習
DLT	Distributed Ledger Technology 分散式帳本技術
DNFBP	Designated Non-financial Business and Profession 指定之非金融事業或人員
DPP	Data Protection and Privacy 資料保護與隱私
EDPB	European Data Protection Board 歐盟個人資料保護委員會
FATF	Financial Action Task Force 防制洗錢金融行動工作組織
FI	Financial institution 金融機構
GDPR	General Data Protection Regulation 一般資料保護規定
MER	Mutual Evaluation Report 相互評鑑報告
ML/TF	Money Laundering/Terrorist Financing 洗錢／資恐
MVTS	Money or Value Transfer Service 金錢或價值移轉服務
NLP	Natural Language Processing 自然語言處理
NRA	National Risk Assessment 國家風險評估
PEP	Politically Exposed Person 重要政治性職務之人
PSCF	Private Sector Consultative Forums 私部門諮商論壇
SSB	Standard Setting Body 標準制定機構
STR	Suspicious Transaction Report 可疑交易報告

執行摘要

1. 近年來科技進步幫助金融機構更有效地分析大量結構化與非結構化的資料同時更有效地識別模式和趨勢。經由彙整資料及運用協作分析，金融機構更能理解、評估和降低洗錢和恐怖主義融資風險，故能更動態、有效即時的辨識此類活動，並幫助私部門以更及時、輕鬆的方式遵守防制洗錢及打擊資恐的要求，亦可防止與多個國內及國際金融機構接觸的犯罪分子利用每個機構對交易之有限與片面觀點的資訊落差以清洗其非法資金。
2. 然而，資料的彙整和協作分析也有可能侵犯對個人和隱私權的保護。因此，任何資訊交流都必須尊重國內和國際間資料保護及隱私法律架構。
3. 本報告承認，防制洗錢／打擊資恐以及資料隱私和保護都是為了實現重要目的之重要公共利益，彼此既非對立，本質上亦未相互排斥。資料保護原則和規則透過國際和國內法律文書實現其保護人權和基本自由，特別是隱私權的目的。本報告指出，為了防止洗錢、恐怖融資、資助武器擴散和其他金融犯罪，法律機制必須以尊重個人的基本隱私權和資料保護權的方式來促成。
4. 新興的強化隱私技術為特定使用情況提供資料保護的方法大有可為，並符合國內及國際資料保護及隱私規範框架。強化隱私技術依靠一系列不同的加密工具於各種情況下實現隱私強化。這些工具使多方能夠在實現應用目標之前提下進行有意義的互動，而不會向對方或第三方透露潛在的私人資訊。此議題的研究和討論領域越來越多，但目前還沒有任何技術標準，所以開發此類標準和開源參考資料的工作仍然很多，這將闡明強化隱私技術可以保護資料隱私的具體使用情況。

5. 這份盤點報告審查了有助於在個別受監管法人實體內進行防制洗錢／打擊資恐進階分析，以及彼此間之協作分析上可用的商用與新興技術，包括對使用這些新技術的預期目標和驅動因素的分析，及考慮或引進此類技術時之政策考量及潛在解決方案。
6. 金融行動工作組將繼續與防制洗錢／打擊資恐的監管單位、技術開發商、金融機構和資料隱私和保護主管機關以及其他有關專家之間進行對話，確保能夠提高防制洗錢／打擊資恐效力的新技術得到充分利用，並符合國內和國際間資料隱私和保護之法律架構。

1. 導論

7. 資料庫和協作分析，是指對不同來源（包括多方）的（數位）資料進行分析的過程。這些資料庫可以集中式（資料庫）或分散式（協作分析）的方式組織起來[1]。本文討論金融機構之間的資料庫和協作分析，包括國際金融集團內部和外部。資料庫和協作分析有好處，但也有一些重大風險。它可以促成強化對洗錢和恐怖主義融資風險的共同理解、評估和緩解的分析工具的使用，從而對這些活動的識別能更加動態、有效和效率。它可以減少誤報的數量，使私部門能夠以更及時、更輕鬆的方式更有效地合規。它可以減少誤報的數量，使私部門能夠以更及時、更輕鬆的方式更有效地合規。它還有助於防止試圖與多個國內和國際金融機構接觸的犯罪分子，利用每個機構對交易的看法都是有限和片面的此資訊落差進行監管套利。然而，這也可能侵犯了對個人和基本權利的保護。因此，任何資訊交流都必須尊重國家和國際間資料保護和隱私權（DPP）之法律架構。

8. 近年來技術進步使金融機構能夠更有效率地分析大量的結構化和非結構化資料同時更有效率地識別模式和趨勢。使用大數據和先進的分析方法，如人工智慧（AI）[2]有可能加強金融部門的防制洗錢／打擊資恐的遵循，但在分享個人資料或程式缺乏足夠的可解釋性同時可能產生偏見或其他錯誤的結果時，也會帶來個人與基本權利的風險。例如，金融機構可以利用先進的分析技術，更準

---

1 對於協作式分析，資料不會被轉移到一個集中位置以便與其他資料一起分析，而是將分析工具帶到資料所在處，不會反其道而行。如此更容易確保資料安全並得以控制存取資料之人、存取資料之內容與目的。

2 關鍵數位轉型定義清單詳附件 A。

確地識別可疑活動、篩選客戶並管理風險。由於進階分析法的準確性主要取決於資料集的規模、品質和相關性，這些工具的功效和效率可能有賴於金融機構（在金融集團內部和外部）分享資訊的能力。

9. 交換、合併或分析資料的技術必須保護個人資訊以符合國內及國際法律架構。因此，對資料分享的需求需要仔細分析防制洗錢／打擊資恐和資料保護與隱私權之影響。例如，金融機構應只收集和處理為實現具體且明確之目的（即目的限制）所必需的個人資料（即資料最少蒐集原則），並且不以與這些目的不相符的方式進一步運用。資訊分享也應該是為了達到特定目的且無法要求以需要較少訪問個人可識別資訊身份之侵入性較小措施來實現，所蒐集資料也不應保留超過必要時間，且不應轉移至無適當資料保護規範之實體。

10. 新興之強化隱私技術為在特定使用情況之資訊提供了有希望的方法，並符合國家和國際資料保護和隱私架構。強化隱私技術依靠一系列不同的加密工具在各種應用下強化隱私[3]。這些工具使多方參與者能夠在實現目標前提下進行有意義的互動，而不會向對方或第三方透露潛在的私人資訊。關於這個問題的研究和討論的領域越來越多，但目前還沒有任何技術標準，所以開發此類標準和開源參考資料的工作仍然很多，強化隱私技術是否在具體使用情

---

3 強化隱私技術包括：同態加密（HE）、全同態加密（FHE）、零知識證明（ZKP）、安全多方運算（SMPC）、功能加密（FE）、群簽和環簽（GRS）、私人資訊檢索（PIR）、私人集合交叉（PSI）、可搜索加密（SE）、盲簽名（BS）、https：//csrc.nist.gov/CSRC/media/Projects/pec /documents/suite-draft1.pdf；基於身份的加密（IBE）等等。見，例如，https：//csrc.nist.gov /projects/pec；https：//csrc.nist.gov/CSRC/media/Presentations/icmc2020-slides/images-media /20200923-PEC-ICMC-slides.pdf；https：//zkproof.org/。

況下提供資料隱私保護將愈加明確。此外，當這些技術的目的是使用資料來識別特定的自然人或法人（例如，導引客戶）時，資料隱私保護可能會受到影響。因此，一些司法管轄區的資料分享倡議目前可能僅限於分享不屬於相關資料保護與隱私權之法定範圍的非個人資料（例如，不包括客戶相關資料的企業資料）。

11. 2020 年 6 月，根據防制洗錢金融行動工作組織（FATF）主席國德國與防制洗錢／打擊資恐數位轉型有關的優先事項，防制洗錢金融行動工作組織同意對資料庫、協作分析和資料保護進行評估。該專案的目的是審查商業上可用的或新興的技術，這些技術有助於受監管實體的防制洗錢／打擊資恐之進階分析或金融機構之間的協作分析，並確定挑戰和潛在的解決方案，以便充分利用這種技術，以強化防制洗錢／打擊資恐之法令遵循，並符合國內及國際間之資料保護與隱私權法律架構。

12. 本報告的組織結構如下：第 2 節介紹防制洗錢金融行動工作組織先前在私部門資訊分享方面的工作背景；第 3 節概述使用新技術進行私部門資訊分享和分析的預期目標和驅動因素；第 4 節概述正在開發或使用的各種新技術；第 5 節列出問卷調查對象在開發或建置這些技術時遇到的挑戰和障礙；第 6 節概述調查對象提出對於更廣泛建置新技術之解決方案（目前尚未得到防制洗錢金融行動工作組織的認可）。

13. 關於本項目的範圍，本文件審查了私對私的資料彙整和協作分析（包括公部門支援或發起之成果）。使用新技術進行公私資訊分享－特別是在報告公司法人實體和金融情報單位／執法機構之間－將在另一份關於業務機構的防制洗錢／打擊資恐數位轉型的文件中進行審查。

2. 方法論

14. 2020 年 11 月，防制洗錢金融行動工作組織向防制洗錢／打擊資恐的國家當局和私部門利害關係人（包括學術界、金融機構和技術開發商）分發了一份關於數位轉型的線上問卷調查用以收集可用於促進協作分析的各種新技術。總共收到了 188 份完整的答覆。本文總結該問卷調查的結果，以及對公營和私部門利害關係人的次級資料研究和訪談，包括來自金融機構、技術開發商、防制洗錢／打擊資恐和資料保護及隱私權之主管機關。

15. 問卷蒐集了利益相關方對使用新技術促進協作分析預期結果之看法，以及如何使用新技術以保護、協作和分析資料。清單內包括與實施此類技術所遇挑戰和政策考慮相關的問題，及與防制洗錢／打擊資恐和資料保護及隱私權監管者接觸的問題。問卷同時尋求個案研究用以闡明 " 回覆者 "（以下指對問卷調查作出答覆的人和秘書處聯繫的專家，包括防制洗錢金融行動工作組織代表團提名的專家）的最佳實務做法。

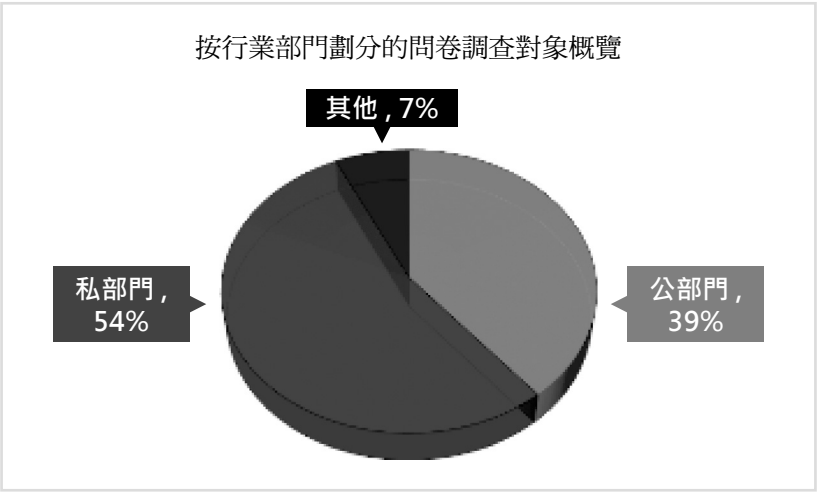
16. 下圖顯示各部門答覆的比例。在公部門層面，大多數回覆者被歸類為監理機關，而在私部門層面，大多數意見來自金融機構和技術開發商[4]。被歸類為“大型銀行“的機構是問卷的主要貢獻者。大多數回覆者位於歐洲（53%），其次是美洲（20%），亞洲／大洋洲（18%），以及非洲（9%）[5]。

---

4 在特指為 " 私部門 " 的回覆者中，54% 為 " 金融機構 "，46% 指定為 " 技術提供商 "。

5 " 其他回覆者 " 為非營利組織、智庫和學術界。

圖 1. 按行業部門劃分的問卷調查對象概覽



3. 背景

17. 對防制洗錢金融行動工作組織而言，資料庫和協作分析並不是一個全新的議題。防制洗錢金融行動工作組織的一些建議包括與私對私資訊分享有關的要件，例如，建議第 18 項要求在金融集團範圍內為客戶盡職調查（CDD）目的和洗錢／資恐風險管理進行資訊分享。這種分享包括對看似異常的交易或活動的資訊和分析（如果已進行此類分析）；並可能包括可疑交易報告（STR）、其基本資訊或提交可疑交易報告的事實。這一要求適用於 FATF 術語表中金融集團定義所涵蓋的所有實體（在國內和跨境環境中）[6]。建議第 21 項進一步確保金融機構及其董事、主管和雇員能夠披露已提交可疑交易報告或相關資訊的事實，只要是符合建議 18 規定的全集團洗錢及資恐風險管理要求。最後，建議第 2 項的措施要求當局合作和協調，以確保防制洗錢／打擊資恐的要求與資料保護與隱私權和其他類似規定相一致　強調當局在解決實際的或觀察到的資訊分享障礙扮演之重要角色。

18. 雖然這些建議概述了在金融集團範圍內分享資訊的細節，但防制洗錢金融行動工作組織的標準目前沒有包括對金融集團以外的資訊分享的類似要求。

19. 2017 年，防制洗錢金融行動工作組織發佈《私部門資訊分享指引》。該指引強調金融機構之間資訊分享的措施，這些措施超越了防制洗錢金融行動工作組織的建議（第 22-25 頁）。此後，這一領域出現了一些區域／國家措施。例如，歐洲聯盟（歐盟）第

---

6 防制洗錢金融行動工作組織術語表將金融集團定義為"由母公司或對集團其他部分行使控制和協調職能以適用核心原則的集團監督的任何其他類型的法人組成的集團，以及在集團層級受防制洗錢／打擊資恐政策和程序約束的分支機構和／或子公司"。

5 號防制洗錢指令中不具約束力的第 46 條規定：「犯罪分子通過許多金融中介機構轉移非法所得以避免被發現。因此，必須允許信貸和金融機構不僅在集團成員之間，而且應與其他信貸和金融機構交換資訊，同時適當考慮國家法律規定的資料保護規則。」[7] 2020 年 12 月，歐洲個人資料保護委員會（EDPB）也通過了一項聲明，特別指出即將修正的立法[8]將解決保護隱私和個人資料與防制洗錢／打擊資恐措施之間的相互扞格，以及它們在實地的具體應用。歐洲個人資料保護委員會指出，它相信在關於防制洗錢及打擊資恐與資料保護及隱私權這兩套規則之間更緊密的銜接，將有利於保護個人資料和提高防制洗錢體系的效率。歐洲個人資料保護委員會重申，根據《一般資料保護條例》（EU GDPR）第 5(1) 條，處理個人資料需要有明確的法律依據，並說明這種處理的目的和限制，特別是關於資訊分享和資料的國際移轉。（歐洲個人資料保護委員會 , 2020, [1]）

20. 隨著各種增強隱私的技術的引進和應用[9]，私部門彙集和協作分析資料上推出了一些倡議和試點方案，包括客戶盡職調查資料，以加強防制洗錢／打擊資恐的合規，更能識別非法活動。這些全球性倡議凸顯了金融機構對合作和集中資源的渴望，及防制洗錢金融行動工作組織在現有指引要解決新技術背景下的資料彙整和合作分析問題上需要更進一步。

---

7 歐洲議會和理事會 2018 年 5 月 30 日第 2018/843 號（EU）指令的第 46 條，該指令修正了關於防止為洗錢或資恐而對金融系統的使用的第 2015/849 號（EU）指令，並修正了第 2009/138/EC 號和第 2013/36/EU 號指令。

8 歐盟計畫以統一防制洗錢法規的形式制定單一規則手冊。

9 強化隱私技術（通常被稱為 PET 或隱私強化型密碼學），是 " 專業的加密能力，它允許在基礎資料上進行運算，而資料所有者不必洩露該基礎資料。同樣之技術可以確保資料所有者對無法得知搜索查詢，查詢和結果仍然是加密的（或不披露），只有請求者能得知 "。（Maxwell, 2020[16]）

4. 私部門防制洗錢及打擊資恐資訊分享和分析之目的與前提條件

21. 防制洗錢金融行動工作組織最近審查了金融機構和金融集團內部和其之間的資訊分享，其範圍較窄，即基於防制洗錢／打擊資恐的目的，在個案基礎上分享具體資訊（例如，審查已觸發紅旗指標的客戶）。本評估報告在此一工作的基礎上，考慮了仰賴大規模私對私資料庫和協作分析的技術創新如何促進防制洗錢、打擊資恐及反武器擴散的目標，同時也符合資料保護與隱私權要求。

22. 在涉及敏感個人資料加密的其他領域如衛生部門測試的新興技術[10]可能提供創新的解決方案，以尊重不同的國家和國際間分歧的資料保護及隱私權相關法律，並允許為防制洗錢／打擊資恐的目的交換和分析資訊。事實上，根據問卷調查的結果，93%的受訪者認為，新技術可能有助於克服防制洗錢／打擊資恐方面及其他資料分享之挑戰（例如，為競爭目的保護專有資訊）。

4.1. 為何要資訊分享？

23. 資料分享對於打擊洗錢、資恐及資武擴活動至關重要。多國的防制洗錢、資恐及資武擴計畫並不考慮國界，犯罪分子也不會只利用一個機構來清洗他們的非法所得。通常情況下，只有當機構和當局能夠檢查一個行為者在不同國家和平台的所有活動時，非法活動才會變得顯而易見。各種國際洗錢案件證明此一觀點，這些案件利用多個司法管轄區的金融機構的弱點，對大量犯罪所得進

10 例如，使用聯合資料（或聯盟式學習）是衛生部門一個增長促進資訊分享和研究合作的趨勢（Tim Hulsen，2020[19]）。

行洗錢。多個機構對所有活動的協調評估可以提高所開發的金融情報的整體品質。

24. 為了更好地防止和偵查濫用國際金融系統為洗錢及資恐的行為，金融機構可以考慮讓金融集團內部以及在不屬於同一金融集團的金融機構之間，在符合資料保護及隱私權要求的情況下進行合作。同時，金融機構應意識到它們可能因違反資料保護及隱私權要求而承擔的責任。一般來說，不建議金融機構分享個人資料，除非這種資料分享的界限（資料類型、分享情況、通信管道等）已由其業務所在之司法管轄區的立法明確規定。

25. 這種資訊分享可以得到當局的支援，但同樣可以在行業層面上進行，而且不一定需要政府的參與，只要法律明確規定了資料合作的範圍和目的，並對私部門的實施進行有效的資料保護監督。

26. 受訪者指出，獲得更廣泛的資料集可以改善結果，並通過減少誤報、推動優先次序、提高金融犯罪調查的效率、改善企業資料品質和提高運營效率，實現以情報為導向的決策。當然，如第 6.2 節所述，資料品質和資料標準化是協作分析整體準確性的重要因素。

27. 對多個金融機構共用的資料進行進階分析，可以揭示趨勢或潛在的可疑活動，否則單一機構可能無法發現。例如，受訪者指出，實體解析和網路分析等工具和技術可以識別聯繫，而在資料零散、調查員所擁有的技術能面向單個機構進行合規檢查時，這些聯繫更有可能被發現。再者，分析技術的使用使金融機構能夠大規模地分析金融犯罪風險，並允許更主動地識別風險。因此，新技術可能會提高所交換資訊的價值和實用性。下面的案例研究提供一個關於英國 2018-2020 年資料共用概念驗證中所取得的好處的例子。

案例 4.1 英國 TriBank 試點方案

2019 年在英國進行的 TriBank 試點涉及三家大型銀行，將假名交易資料（即日期、金額和記號化的發送方和接收方帳戶）結合起來，以便進行整體分析。參與銀行沒有披露個人資訊（如姓名和位址）。試點專案證明，假名交易資料可以安全有效地從多個參與的金融機構收集，可以合併和連結成一個有意義的統一資料集，並進行集中分析。該技術平台顯示，在不瞭解基本交易帳戶的情況下，可以自動識別大型和複雜的集群，從廣泛的帳戶基礎中挑選出來，並將其作為參與機構進一步分析的候選人。

該試點項目展示了兩種互補的防制洗錢／打擊資恐合作分析方法。1）參與的金融機構提供有關可疑、關注帳戶的初始資訊，而平台則大大擴展了這種重要的情報，以顯示＂全貌＂；2）平台本身自動識別值得關注的區域，而無需金融機構提供任何重要的情報。這兩種方法相輔相成，創建了一個有效的跨銀行交易監控體系，使每個參與機構都能貢獻自己的情報，並從其他機構的情報中獲益，而任何人都不必披露任何機密的客戶資訊。

28. 一些受訪者還指出，在一些地區，隨著金融科技公司和其他新的銀行業市場參與者的出現，客戶正在遠離現有的傳統銀行，並使用多個機構進行銀行業務，而不是在擁有高市占率的單一金融機構進行銀行業務。這意味著關於個人客戶的資料正越來越多地分散在眾多金融機構中，從而使得僅根據單一機構的資料獲得洗錢及資恐之洞察力變得更加困難。這進一步刺激了私人機構之間的資料分享和合作，以便彙集足夠的資料庫，應用先進的分析方法，更準確地評估客戶風險或識別潛在的可疑活動。

29. 然而，資料處理程序必須與追求的合法目的相稱。在處理的所有階段，必須保證所有相關利益和權利之間的公平平衡。確切地說，個人資料必須以透明的方式公平處理，並為明確、具體和合法的目的收集，同時遵守資料保留規則。資料分享和技術運用的各方面，包括防制洗錢／打擊資恐的有效性和資料保護及隱私權及競爭影響，應首先進行評估，以便在項目建置前各方面已適當考量。

4.2. 私人對私人資料庫分享倡議之既定目標為何？

30. 雖然不是一份詳盡的清單，但金融機構可以決定分享資料，包括與其他金融集團和甚至跨過不同的司法管轄區分享資料，有利於：

▪ 執行客戶盡職調查措施，例如

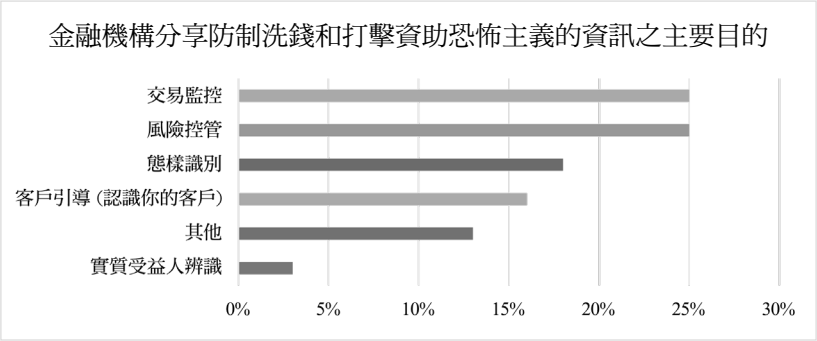
- *機構風險評估：*更準確地衡量洗錢及資恐之風險，以便為新產品和服務採取更好的衡量標準。
- *客戶引導*：確定一個自然人或法人以前是否在金融集團內外的另一個機構被提出警告或關切；通過檢查各業務線是否存在類似行為來核實客戶之風險等級。
- *交易監控*：通過檢查客戶的交易模式以評估財務狀況來發覺多層化隱匿，對跨機構檢測到的任何異常活動進行追蹤、更好地識別可疑活動、應用交易門檻。
- *業務關係之風險管理*：持續更新客戶資訊、識別在多個金融機構引入同一客戶時產生的全球風險、動態風險管理以反映新的資訊或客戶行為的變化。
- *受益人之識別*：提高識別受益人的準確性、識別在不同機構之同一受益人、加強對空殼公司的偵測、開發一個更有效率的受益人資訊之記錄管理系統。

▪ 端對端的技術流程，例如。

- ***犯罪態樣之識別***：更迅速且更準確地識別新興犯罪態樣及施行保護措施，同時與其他機構和公部門分享調查結果。
- ***情報推動的調查***：調整調查工作以得出更完整可靠的調查結果。

31. 根據調查表的結果，為防制洗錢／打擊資恐的目的分享或彙集資料的主要原因是為了監控交易。然而，一些回覆者指出，這種舉措的目的可以包括上述清單中的多種選擇。下圖總結了對調查問卷的答覆，其中確定了金融機構分享防制洗錢／打擊資恐資訊的各種目的。

圖 2. 金融機構分享防制洗錢及打擊資恐資訊之主要目的



表格說明：受訪者只能從中選擇一個答案。

32. 分享防制洗錢／打擊資恐資訊中的 " 其他理由 " 的例子包括：

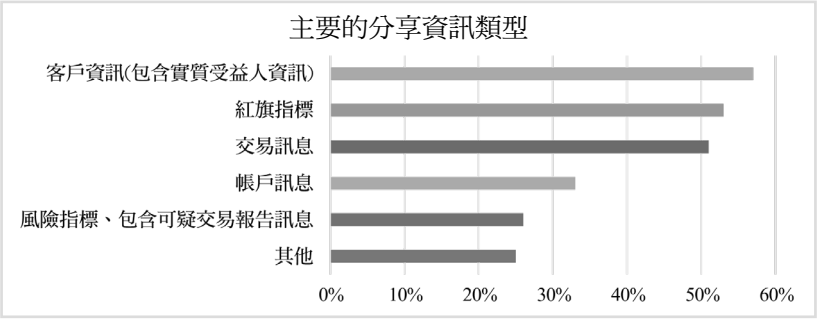
- 減少風險，以便在偵查、預防和調查防制洗錢／打擊資恐方面做出更好的決策，更普遍的是；
- 促進反饋迴路，以開發和優化資料處理參數。
- 開展以情報為導向的調查；以及
- 促進發展資料驅動之犯罪態樣。

4.3. 資訊分享之類型？

33. 為實現上述具體目標，加密的分享資料可包括： 客戶盡職調查資訊；交易資料；紅旗指標；客戶風險指標，如是否已提交可疑交易報告；以及通匯銀行關係中各機構的最新資訊，包括可促進各機構進行風險評估和持續盡職調查的客戶資訊。

34. 根據問卷調查的結果，（目前或正在考慮）分享資料的主要類型是客戶資訊（包括實質受益人資訊）、與紅旗有關的資訊和交易資料。受訪者指出，根據倡議的具體目標，通常會分享各種資料類別的組合。然而，一些受訪者還指出，客戶資訊的分享只會在加密狀態下和在有限的概念驗證背景下發生。下圖總結問卷調查之結果，以確定問卷調查受訪者目前分享或正在考慮的主要資訊類型。

圖 3. 主要的分享資訊類型



表格說明：受訪者可以選擇所有選項。

35. 分享的 " 其他類型資料 " 包括：
    - 法人機構識別碼（LEI）[11] 參考資料；
    - 態樣；以及
    - 警報處置、結果（以內部模型調整）。

[11] 法人機構識別碼（LEI）為由數字和字母組成的 20 位元編碼，能夠清楚和獨特地識別參與金融交易的法人實體。欲瞭解更多資訊，請參閱 " 法人機構識別碼（LEI）簡介 "，全球法律實體識別碼基金會（GLEIF），www.gleif.org/en/。

案例 4.2. 日本的機器學習和人工智慧概念驗證

日本為了促進與資料保護及隱私權法規相一致的資料分享，開發了一個獨特的概念驗證（POC）專案，該專案由日本金融服務機構支援，由新能源和工業技術發展組織贊助，包括幾個日本金融機構的參與。這個專案將人工智慧演算法與每個金融機構交易資料集的指令整合在一起，不需要分享或彙集資料，從而形成一個單一的人工智慧模型。

這個概念驗證的目的是建立一個人工智慧模型，通過計算交易監控和制裁篩選的真實陽性分數的可能性來幫助人類的判斷。

在這個概念驗證中，並未分享或彙整各個金融機構的交易資料，而是採取以下兩種方法：（1）整合了學習各機構資料庫的人工智慧模型本身；（2）調整已經學習了一家機構資料集的人工智慧模型以重新學習另一家銀行的資料集，並重複這一過程以提高這個人工智慧模型的準確性。

根據這個專案的成果，帶有人工智慧的分享交易監控和篩選系統有足夠的潛力來減少工作量，包括檢測之分類過程和處理偽陽性。在準確性和可解釋性方面顯示，傳統分類過程中的一些人為操作可以被人工智慧的判斷所取代。如果這一計畫推廣到更廣泛的金融業參與者，它可以提高整個防制洗錢／打擊資恐的效率和效果。

4.4 使用新技術之驅動因素及前提條件

36. 本節概述為防制洗錢／打擊資恐目的而運用私對私資料分享和協作分析新技術之現狀，以及有利發展及建置此類技術的環境、驅動因素與先決條件。

37. 根據問卷調查結果，只有 40%的回覆者表示，其司法管轄範區之金融機構正在利用新技術與其他金融機構分享或彙集資料以達到防制洗錢及打擊資恐的目的。在這些回覆者中，有 72%表示，此一措施是由公部門和私部門共同制定的。

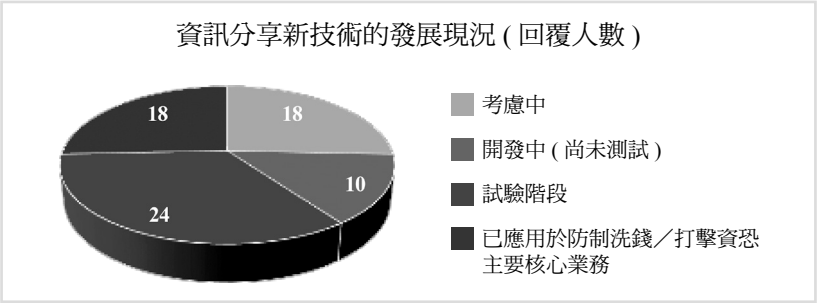
38. 以下案例研究係共同開發私對私防制洗錢／打擊資恐資訊分享安排模式之例子。

案例 4.3. 中國的資訊分享平台試驗

在中國人民銀行防制洗錢局的指導和監督下，幾個中國金融機構正在試運行一個整合區塊鏈、數位身份和可靠的強化隱私技術之防制洗錢風險資訊分享平台（以下簡稱＂資訊分享平台＂）。該資訊分享平台允許參與的金融機構對高風險客戶資訊進行加密，包括數位身份號碼（DID）和機構標明之風險標籤，然後將其上傳至區塊鏈上。當參與機構查詢客戶時，通過安全運算平台在區塊鏈上進行匹配。只有當且僅當該被查詢個人的姓名和國民身份證號碼被其他參與機構上傳時，數位身份號碼才會被匹配。匹配後，資訊分享平台提取洗錢風險資訊，並以密碼文本形式回傳以待解密；處理單位也立即刪除此類運算的任何記錄。然後，會提醒查詢之金融機構某人在另一金融機構也是高風險，或被其他金融機構查詢。因此，在這個項目設計中，機構之間沒有實際的客戶資料交換。

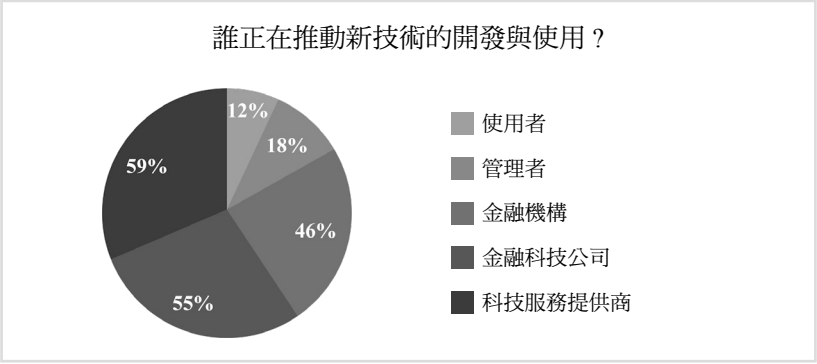
39. 問卷調查的答覆還顯示，使用新技術促進私營機構間協作分析和資料彙集的大多數計畫目前處於開發和測試之初級階段。例如，大多數受訪者（74%）指出，此類技術的部署階段不是仍在考慮中，就是處於開發或測試階段。下圖概述對這些新技術當前部署階段的問卷調查的答覆。

圖 4. 資訊分享新技術的發展現況



40. 如下圖所示，受訪者指出，測試和使用新技術進行資料彙集和協作分析的各種計畫是由私部門推動的，特別是大型跨國金融機構、零售和商業銀行以及網路公司（金融科技和其他）。

圖 5. 開發與使用新科技的推動力



表格說明：受訪者可以從中複選答案。

41. 使用新資料分享技術的其他驅動因素包括：有望提高防制洗錢／打擊資恐的效力和效率的技術發展的出現，以及建立有利和明確的監管體系，以部署私營機構之間的資料分享新技術。

42. 在一些司法管轄區，防制洗錢及打擊資恐的監管者與私部門密切合作，鼓勵開發防制洗錢及打擊資恐協作分析和資料彙集的新方法和技術。一些回覆者特別指出，在開發新項目時，會諮詢防制洗錢及打擊資恐的監管者和主管個人資料隱私權保護之部門。私部門指出，與監管者和主管部門的公開對話對運用新技術的計畫取得成功以及最終有效實施至關重要。

43. 在某些情況下，修法是實施私營機構協作分析技術的先決條件。因此，在這種情況下，防制洗錢／打擊資恐的政策制定者和防制洗錢／打擊資恐的監督者的參與，是這些計畫成功的必要條件。下面的案例研究概述了一項由私部門主導的彙集防制洗錢／打擊資恐資料的倡議，該倡議需要為其未來技術實施進行修法。該案例研究顯示各主管部門和私部門參與者之間公開對話的重要性。

案例 4.4. 荷蘭交易監控 （TMNL）

TMNL 荷蘭交易監控是五家荷蘭銀行的聯合倡議，旨在聯合監控其支付交易以辨識洗錢或資恐指標的信號。在撰寫本報告時，荷蘭交易監控之實用程式正在建置中。

經由對合併交易資料的聯合交易監控，其主要目標是藉此識別個別銀行無法單獨察覺的異常交易模式，提高對洗錢活動的偵測。因此，荷蘭交易監控將專注於所謂的多銀行警報。除了這個聯合監控平台外，參與銀行還將繼續持續監控自己的交易，以符合荷蘭反洗錢法規的要求。

所彙集的參與銀行之交易資料庫將只涉及在荷蘭國內管理的銀行帳戶上執行之交易。長遠來看，可以預期其他銀行也會加入荷蘭交易監控。一旦投入運行，如果荷蘭交易監控標記為推測存在洗錢或其

他非法活動的潛在之異常交易或一系列轉帳，支付鏈上所有參與者將收到與該交易有關的警報。接收銀行將獨立審查來自荷蘭交易監控的警報，並獨自決定是否向荷蘭金融情報機構提交異常交易報告（是否申報的決定則不會在平台上分享）。在撰寫本報告時，該專案主要關注與企業客戶有關的交易資訊。

荷蘭交易監控目前正在建構用以接收所有交易資料所需的平台，將它們結合起來進行聯合交易監控，並向參與銀行通報推測之多個銀行異常警報。該平台建立在雲端上，同時在其中一家參與銀行在的所謂加速器平台建立備份。此一量身定製之平台的設計原則之一是模組化的設置，允許使用最先進的工具來推進。銀行和荷蘭交易監控之間交換的隱私敏感交易資料將被匿名化。

為了開發這個專案，參與的荷蘭銀行一直在與政府合作夥伴密切合作，如資料保護局、財政部、司法和安全部、國稅局、調查局以及金融情報機構。荷蘭交易監控的成立與荷蘭政府宣佈的 2019 年洗錢行動計畫互相呼應。作為該計畫的一部分，預計將對《反洗錢／反資恐法》進行修訂，以實現全面的集體交易監控[12]。該修正案旨在使荷蘭的銀行能夠分享更多的交易資料和推定的異常交易資訊，解除交易監控程序外包的禁令，並允許在聯合交易監控過程中使用公民服務編號，即獨特的私人個人身份號碼。

44. 除了金融機構與防制洗錢及打擊資恐及資料保護和隱私權相關聯之國家當局間的公開對話外，受訪者還注意到監理沙盒（或新創中心）在測試新技術如何與國家（或超國家）防制洗錢／打擊資

12 在撰寫本報告時，允許荷蘭交易監控的法規仍在研擬中，尚未提交給議會。

恐和資料保護和隱私權法律和法規互動的價值。然而，正如聯合國秘書長普惠金融特別倡議（UNSGSA）之金融科技工作組最近發表的報告所概述，監理沙盒的建立可能很複雜，運行成本同樣很高[13]。

45. 問卷受訪者指出，沙盒和創新辦公室或創新中心被強調為既是驅動力又是有利環境，因為它們通過協助參與者確定機會、風險、脆弱性和抵減措施，促進和鼓勵新方法的開發和實施。下面的案例包括監理沙盒和新技術創新中心的例子，以分享防制洗錢／打擊資恐的資料。

案例 4.5. 可行之監管環境

英國

金融行為監管局（FCA）在 2019 年舉行了一次科技黑客松（TechSprint）活動，研究被稱為隱私強化技術的加密技術，如何促進有關洗錢和金融犯罪的資訊分享，同時遵守資料安全法規。這次活動包括來自行業內的代表，展示他們的措施、技術以及取得的成果，反洗錢監管人員和英國資訊委員辦公室（ICO）亦派代表出席。金融行為監管局最近開展了數位沙盒試點，為希望開發新的解決方案和產品以打擊欺詐及其他詐騙的創新公司提供一定的支持，包括存取模擬的銀行交易資料庫。其中一些公司在開發這些解決方案時採用了強化隱私技術。該試點於 2021 年 2 月結束，並將供未來迭代之數位測試環境參考。

13 聯合國秘書長普惠金融倡議（UNSGSA）的金融科技工作組和劍橋大學新興金融研究中心（CCAF）.（2019）. 監理創新實現惠普金融科技的早期經驗：創新辦公室、監理沙盒和監管科技。UNSGSA 和 CCAF：紐約州紐約市和英國劍橋市。

法國

法國金融審慎監理總署（ACPR）創建了一個金融科技創新中心，以連接創新金融生態系統。這個專門的精實團隊，發揮創新觀察站的作用，對所有創新項目持有者開放。它還負責金融審慎監理總署內部的＂監理科技＂工作，即在監督工作中整合新技術。金融審慎監理總署的金融科技創新中心在過去兩年中領導四個與反洗錢和打擊資恐有關的工作組。這些工作組聚集了產業代表和公共機構（金融情報機構、安全和資料保護機構），討論了諸如遠端確認客戶身分、虛擬資產部門的防制洗錢／打擊資恐流程等問題、及以反洗錢視角檢視銀行與虛擬資產服務提供者之間的關係。此外，金融審慎監理總署金融科技創新中心還與學術界就金融業新技術的機會和監管挑戰進行了對話。在此背景下，審慎管理局於 2020 年 3 月舉辦了一次以資料分享和資料庫為議題的研討會，會中強調前沿技術如何在無需分享資料的情況下實現知識分享。例如，差分隱私所提供的隱私保證可以用來訓練預測模型 -- 例如那些嵌入交易監控系統的模型—處理過於敏感而無法對任何金融機構揭露之資料。然而，另一項技術是安全多方運算，這是一個安全協作過程的構件，例如根據來自多個金融機構的交易和使用者資料庫，產生關於國際銀行詐欺帳號的關鍵績效指標。

46. 最後，受訪者還強調，在開發資料庫和協作分析的新技術時，需要進行徹底的資料保護影響評估。在一些國家，這種評估是資料處理前以最大限度地減少對個人權利的確認風險之監管要求。

5. 識別防制洗錢及打擊資恐資訊共享與分析之新技術

47. 本節概述了目前正在開發或使用的各種新技術，以促進金融機構之間為防制洗錢／打擊資恐而進行的資料分享和分析。這些新技術是在次級資料研究和與受訪者訪談過程中得知的。

5.1. 現有之私對私資訊分享技術

48. 下表總結了可能促進私對私的協作分析和資料庫之各種新技術。被提及最多的用於資料合併和協作的技術是密碼學，用於分析大型資料庫的技術是機器學習。然而，調查問卷的受訪者經常指出，資料分享和分析需要使用多種類型的技術，以保護和分析大型資料庫，並確保其符合國內和國際間資料保護及隱私權要求。因此，下表中概述的各種技術經常被一起應用，以確保資料安全和保護。

表 **5.1.** 用於私對私防制洗錢／打擊資恐的協作分析技術之總結

技術類型	描述	防制洗錢／打擊資恐資訊分享之潛在益處之案例
密碼學／加密學技術		
同態加密	此項技術允許機構交叉匹配和搜索第三方資料庫，而不用識別搜索的內容或損害基礎資訊的安全性或所有權。這意味著不同機構可以就機敏資訊進行合作，同時保護隱私、保密性和監管合規。（Microsoft，2016[2]）	因能夠獲得更多的資訊，從而改善產出結果，同時通過減少誤報以實現情報導向之決策，提高金融犯罪調查的效率，改善企業資料品質，提高運營效率。
零知識證明	基本上零知識證明是發生在證明者和驗證者之間的一種加密方法和驗證方法。證明者能夠向驗證者證明他們擁有資訊，而無需披露基礎數據或資訊本身。	該技術允許銀行 A 確定銀行 B 是否持有某個人的資料，而無需分享他的身份。
安全多方運算（SMPC）	安全多方運算使多方能夠對來自不同資料來源的隱私資料進行評估，而不需要彙整或分享資料。在協定結束時，大家除了函數的值其他都無從得知。（Scheibner, 2020[1]）	這項技術可以應用於分散的資料來源，設法從不同方獲得合理懷疑，同時保持資料的主權。
差分隱私	涉及加密協議，允許各方與不同方合作時，對其集體輸入之所有訊息進行聯合運算時保持其自身資料的匿名性。	此科技可能在資料精準度和隱私之間予以權衡，這可能意味著該項科技會更適合分析廣泛趨勢，而非偵測異常或詳細型態。

技術類型	描述	防制洗錢／打擊資恐資訊分享之潛在益處之案例
進階分析		
機器學習（被監督、無監督和強化學習）	為人工智慧之子領域，讓電腦在接觸新資料時能夠學習（通過學習演算法），而非以明確程式設計來執行特定任務。	監督學習方法可用于開發基於歷史驗證／審計結果之合規風險評分模型。 業務流程中的決策點由機器學習模式進行優化以理解當前狀態和預測最佳決策。 評分模型或分類模式可用藉由金融交易或其他相關資料中識別可疑的網路或法人實體。
聯盟式學習	聯盟式學習是一種機器學習技術，它在包含本地資料的多個分散的資料庫中訓練一種演算法。該演算法在各個無相互連結之資料庫且無需交換或移動資料下學習到新資訊（如趨勢）。（Shiffman, 2020[2]）	例如，旅行演算法可以在不移動資料的情況下讀取和查詢不同金融機構的資料庫。其目的是讓演算法學習新型的犯罪趨勢和技術，如果它只停留在單一機構中，就無法學習。這導致了需要更多的動態風險評估工具，如動態紅旗指標。
深度學習	深度學習是機器學習中的一個領域，它使用多層之學習演算法，從大量資料中萃取意義。	可以應用於金融機構，如交易監控。

自然語言處理	自然語言處理讓電腦用他們自己的程式語言與人類交流，並完成其他與語言有關的任務。例如，自然語言處理使電腦有機會能閱讀文本、聽到語音、理解它、衡量觀點和確定哪些部分是重要的。（SAS, 2020[3]）	例如，可以應用於將可疑交易報告中的文本轉化為可用於網路分析的結構化資料。 利用文本探勘，對可疑交易報告或任何文件自動加上註解，以便日後檢索。
機器人流程自動化	軟體自動化技術，" 機器人 "（例如軟體程式）根據人類行為進行程式設計，以模仿這種互動來執行大量的重複性任務，在龐大數量下依然迅速且準確。	高效率地完成以前由人工執行的重複自動化任務。
網路分析	網路分析是利用網路資料來檢測大型資料庫中可能被掩蓋的趨勢和模式。它讓錯綜複雜的實體網路及已識別之關聯屬性得以顯現。	導出在終端層級無法以其他方式看到的模式。 網路分析可用於辨識相關主題之關聯實體網絡。
處理和轉移的基礎設施		
可信的執行環境（機密運算）	機密運算是通過將訊息處離隔離在一個可信執行的硬體環境來保護使用中之資訊。這個環境藉由一部分加密的處理器和記憶體來保護。（Microsoft Azure, n.d.[4]）	例如，雙方同意分享他們的資訊（如交易資料），並使用一個可信的執行環境對其進行分析。

技術類型	描述	防制洗錢／打擊資恐資訊分享之潛在益處之案例
安全的雲端技術	雲端運算是通過網路提供資訊技術服務，讓企業和政府能夠加快創新和協作。雲端運算安全涉及確保雲端運算環境免受外部和內部的網路安全威脅之應用程式和技術。（McAfee, 2020[5]）	雲端技術的進步使企業能夠以非常低的成本收集、存儲和分析大量的資料。這項技術允許存儲和分析結構化和非結構化的資料，同時可用於促進進入受保護雲端環境之間各方的合作。 然而，無論兩個金融機構的資料是否在同一個雲端環境中，資料分享的法律障礙仍然是不變的。
分散式帳本	它是一個加密的、由網路中各方參與者維護的共有交易帳本。由於沒有單一的中央機構控制帳本，它是一種極其安全且透明的資訊儲存方式，將資訊按時間順序存儲在一個原則上不可改變的記錄裡。（OECD, n.d.[6]）	例如，它能在沒有任何一方有能力將資料銷毀的情況下作為一種在多方之間分享資訊的方式。然而，資料分享的法律障礙仍然存在。
應用程式介面（API）	應用程式介面是一個讓受監管機構提交資料的介面。它通過整合資料產出流程提高自動化及降低申報成本，促進受監管機構與主管當局之間的溝通。（FSB, 2020[7]）	允許更有效地收集、存儲和分析大型資訊。

49. 以下案例研究提供正在使用或開發的新技術的例子，以促進金融機構對防制洗錢／打擊資恐之協作分析（其他監管科技案例研究詳附件 B）

案例 5.1. 聯盟式學習

一個由硬體技術提供商和軟體供應商組成的團隊正在努力推出一個機器學習模型可以在多個資料庫上進行訓練的安全的聯盟式學習平台，用以偵測和分析＂正常＂和＂異常＂模式。在這些平台中，模型在不同地點的資料庫中移動，而資料從不移動。這使得該模型能夠根據參與機構的資料庫學習新的犯罪趨勢和技術，同時保護隱私和安全。然後在模型內獲得的知識可用於持續完善和調整各參與機構的風險指標。

案例 5.2. 安全多方運算技術

監管科技開發了一項技術，經由加密處理之確認客戶資料及交易行為與登錄資訊，使兩個或多個金融機構能夠協同運算風險評估功能，而不會暴露上述資訊。這種風險評估功能是運用強化隱私技術來執行並且不需要機構以任何方式或形式實際分享或暴露客戶資料。該技術運用多方運算協定來處理每個機構的資料，而不會將資料暴露在該機構之外。參與機構只交換隨機的字串，不包含客戶資料。關鍵點是，在運算時任何一方都不會向另一方披露資訊。安全多方運算故意模糊運算過程，所以資訊看似沒有被揭露而其結果仍然可以就如同資訊是被直接分享一樣被運算出來。這項技術可以在交易實際發送前執行，或者在反洗錢監測和分析階段執行。該技術還在每個金融機構留下了加密之審計存底。一個外部審計員在得到所有交易客戶的審計存底後，可以重建整個決策過程。

案例 5.3. 同態加密

監管科技為金融機構開發了一個科技輔助靈活且適應性強的信任架構，能夠促進可靠且隱密的確認客戶（KYC）和客戶盡職調查流程，以強化情資導向之決策。該計畫利用獨特之同態加密技術，使資料處理過程一直保持加密，如此一來金融機構能夠安全地搜尋、分享和與第三方資料庫合作時不會洩露搜索內容本身或損害基礎資料的安全性或所有權。在這種分散式資料模型中，參與者永遠不需搬動或整合資料庫。資料所有者保持對其資料的控制同時還能管理存取權。

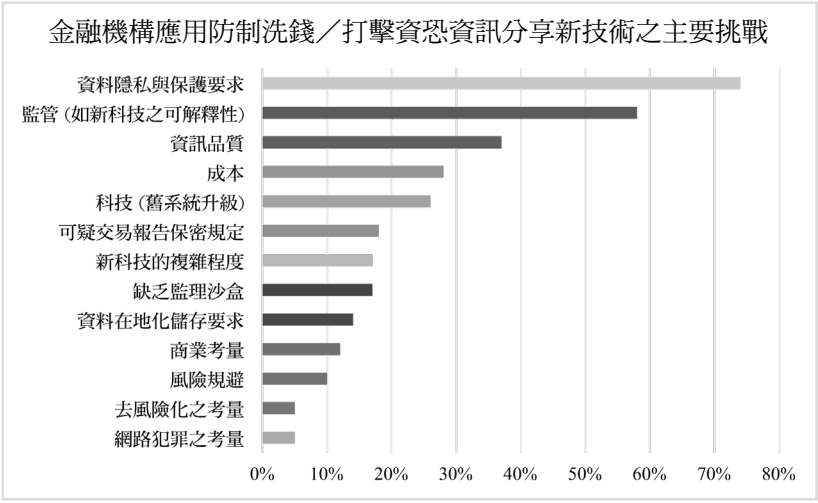
在這種模式下，確認客戶的資訊在不同且可信的參與者或管轄區之間，允許彼此持有的資訊經由加密搜尋並得到驗證，而無需移動或合併資料。分析師能在業務相關的時間範圍內安全且隱密地交叉匹配和搜尋跨境之隱私管制資料，並確保敏感資產在處理過程中按照監管要求得到保護。該解決方案驗證了創新加密技術的應用如何解決金融領域的關鍵挑戰，使企業能夠分享敏感資訊，更瞭解客戶風險，並做出更快、更明智的決策來應對現實世界中防制洗錢和金融犯罪的挑戰。

6. 利用新技術進行資料協作分析之挑戰

50. 金融機構之間特別是跨國並與第三方的資料合併和協作，引起一些政策疑慮。雖然上述 2017 年防制洗錢金融行動工作組織關於私部門資訊分享的指引中曾概述過部分挑戰，但在當利用隱私強化技術和人工智慧等先進的分析方法試圖處理更大的資料庫時，仍會有更多疑慮。

51. 根據調查問卷的結果，資料保護及隱私權要求被認為是開發和應用私對私分享新技術時的首要政策考慮。如下圖所示，其他被高度提及的挑戰包括監管挑戰（包括新技術的可解釋性／可理解性；及激勵措施的缺乏）；以及資料品質（包括缺乏資料標準化）。

圖 6. 金融機構應用防制洗錢／打擊資恐資訊分享新技術之主要挑戰



表格說明：受訪者可以從中選擇最多四個答案。

52. 下文根據對問卷調查的答覆、訪談和研究發現，詳述與資料庫和協作分析有關的挑戰和障礙。

6.1. 確保並強化資料保護及隱私

53. 防制洗錢／打擊資恐和資料保護與隱私權都是為重要目標服務的重大公共利益，既非對立的，本質上亦非相互排斥[14]。資料保護原則和規範透過國際間和國內法律文件實施，旨在保護人權，特別是隱私權等基本自由。最重要的是，法律制度應促進這兩種公共利益，以防止洗錢、資恐和資武擴以及其他金融犯罪同時重視個人的基本隱私權和資料保護權。因金融資料可能包括一些關於個人的最敏感性資料，揭示他們的財務狀況、家庭互動、行為和習慣、健康狀況等。因此，必須考慮防制洗錢／打擊資恐和資料保護及隱私權並以平衡的方式權衡，以符合會員國在國際法（包括人權法）下之義務。根據這些法律，最關鍵的要求之一是確保存在處理個人資料的有效法律依據。此外，必須尊重實現相同目標的替代措施方面的相稱性。下面的案例研究強調了《自動化處理個人資料保護公約》（CETs 第 108 號）中的此類要求，該公約於 1981 年 1 月 28 日開放供簽署，是資料保護領域中第一個具有法律約束力的國際指引書類。

14 例如，根據世界人權宣言和公民和政治權利國際公約，以及在區域級的歐洲人權公約，隱私權是一項基本權。

案例 6.1. 自動化處理個人資料保護公約（第 108 + 號公約）

根據第 108+ 號公約，個人資料的處理可以基於：（1）當事人對處理她／他的個人資料是基於自由意識、確切、知情、明確的同意；或（2）基於法律規定的其他合法基礎（如履行契約、公共利益、確保公共安全、資料控制者之合法利益等）下進行處理（包括獲取）資料。無論是否需要當事人同意，公共利益或合法利益作為有效的法律依據，來自防制洗錢／打擊資恐、資料保護及隱私權和人權領域的國際利益相關者都應仔細分析和闡述其基本原理。

正如第 108+ 號公約第 11 條所概述的，必須明確定義每一類分享的資料，及其處理目的。確定資料可以保留之時間以及對尊重私人生活權利之干預是否適當合理亦有必要。此外，第 6 條規定，為了防止對資料主體的不利影響，為合法目的處理敏感性資料必須有適當的額外保障措施：例如，當事人之明確同意、涵蓋此情況之明確法律規定、專業的保密義務，以及特定的技術安全措施（如資料加密）。

54. 如上所述，洗錢和資恐活動往往涉及多個機構及司法管轄區。為了更能識別可疑行為和降低對金融系統的濫用，金融機構從收發與其客戶包括跨國界有關的資訊和分析中得到改善。金融機構還可能希望處理更大的資料庫，以完善其對新興犯罪趨勢和態樣的理解。同樣地，金融機構也有法律義務保護其客戶的個人資料。

55. 在履行防制洗錢／打擊資恐義務或制定私部門資訊分享計畫時，不同司法管轄區的國內、國際間不同的資料保護及隱私權法律可能會給金融機構帶來挑戰。如果沒有足夠的監管指導或對防制洗錢／打擊資恐的要求和資料保護及隱私權義務採取不一致的做法

時，問題可能更加複雜。不同資料保護及隱私權處理方法的複雜性影響到私部門的資訊提供、獲取、處理和分享。

56. 一個在研究過程和問卷調查的答覆中發現的私對私資料分享和合併重大挑戰是金融機構希望藉著分享資訊以提高遵循防制洗錢／打擊資恐的效率和效力，與現有法律旨在保護客戶隱私，兩者之間存在感知之衝突。在許多司法管轄區，由於資料隱私要求，金融集團對外的分享受到限制。相反，在一個司法管轄區（美國）內，存在允許不屬於同一金融集團的金融機構之間分享防制洗錢／打擊資恐資訊之豁免或 " 安全港 "，如下文範例所示。

案例 6.2. 美國愛國者法案第 314（b）條

美國愛國者法案第 314（b）條（金融機構之間的資訊分享）規定，兩個或多個金融機構和任何金融協會可以自願地相互分享有關涉嫌恐怖份子或洗錢活動的個人、法人、組織和國家的資訊。金融機構或協會在為識別和報告可能涉及恐怖行為或洗錢活動而傳送、接收或分享此類資訊時，不應根據美國聯邦的任何法律或法規、任何州或其從屬政治單位的基本法、法律或法規，或是根據任何契約或其他可依法執行的協定（包括任何仲裁協定）告知該被披露或是應披露而未披露的當事人，或是去告知在申報時被辨認的任何其他人。（FATF, 2017[8]）

關於第 314（b）條安全港之適用，金融機構或協會要有合理的理由相信所分享的資訊與可能涉及洗錢或恐怖活動有關，並且是為了第 314（b）條及其實施條例規定的適當目的而分享資訊即可。因此，金融機構或協會可以分享與其懷疑可能涉及洗錢或恐怖活動的活動有關的資訊，即使該金融機構或組織無法確定特定非法活動中被清洗的具體收益。（FinCEN, 2020[9]）

57. 問卷調查的結果指出，受訪者大多認為，新技術可以解決之前與私部門資料分享時遇到的問題，同時尊重基本權和個人之資料保護及隱私權。許多受訪者還特別呼籲制定國家和國際規則，以釐清何時以及出於何種目的（以及何種類型的資料）可以在金融機構之間為防制洗錢／打擊資恐之目的而分享或匯集，特別是在金融集團之外分享資訊。此外，受訪者指出，當目的是利用資料來識別特定的自然人或法人時，例如在引導客戶時，全新的技術與發展中的技術應用並不保護隱私。

58. 雖然可能需要全球資料保護標準來促進數位合作，但目前沒有任何組織被授權協調其發展。相反，這些標準是在國家和超國家範圍內制定的，因為各國政府負責在其管轄範圍內建立資料保護及隱私權之法律架構。因此，對於金融機構之間可以分享的資料和資訊的種類（即使用於協作分析）缺乏指導，以及上述新興和發展中的技術和流程是否能使組織保持符合國家和超國家的隱私要求也都不明確。

59. 根據聯合國貿易開發委員會的資料，194 個國家中有 132 國已經頒佈了某種形式的立法，以確保資料和隱私的保護 （UNCTAD, 2020[10]）。儘管如此，各國的保障措施和遵從資料保護及隱私權的程度有很大差異。歐盟一般資料保護條例的生效，不僅協調了歐盟和歐洲經濟區間資料保護及隱私權規則，而且還成為世界上許多國家考慮引入現代化隱私規則的催化劑。

60. 下面的案例研究介紹了歐盟的資料保護規則。

案例 6.3. 歐盟的資料保護規則

隱私權和資料保護權被寫入歐洲聯盟基本權利憲章（第 7 條和第 8 條）。

2018 年 5 月 25 日生效的歐盟一般資料保護規則規範了公司如何處理個人資料。除了其他事項，一般資料保護規則要求公司只收集和處理必要的個人資料（即資料最少蒐集原則），以實現特定和明確的目的（即目的性限制），並且不以與不符這些目的之方式進一步處理。它還要求個人被告知他們的資料何時被收集以及資料將被處理的目的。它列出了允許處理個人資料的法律依據的限制性清單並建立了一套個人權利，包括使用、修正和刪除的權利以及不接受僅基於自動處理 (包括分析) 的決定之權利。

一般資料保護規則由每個歐盟成員國的資料保護主管機關（DPA）監督和執行。歐盟個人資料保護委員會由每個資料保護主管機關的代表和歐洲資料保護監督員組成，確保一般資料保護規則於整個歐盟範圍一體適用。

傳輸個人資料至第三國或國際組織應受非常明確之條件限制，以確保一般資料保護規則之保障的不被破壞。特別是，當第三國的資料保護水準基本上等同于歐盟保障的水準時，可以基於歐盟委員會通過的 " 適足性認定 " 而進行傳輸。

重要的是，一般資料保護規則指出，資料保護原則不適用於匿名資料（即資料主體以無法或不再可識別的方式匿名提供個人資料），這不屬於其規定的範圍。另一方面，匿名資料（即在沒有額外資訊的情況下已無法歸屬於特定資料主體的個人資料）被視為個人資料，屬於一般資料保護規則的範圍。

61. 雖然每個司法管轄區的資料保護及隱私權法律可能有所不同，但有趨於一致的趨勢。例如，現在的趨勢是採用具有類似關鍵特徵的資料保護架構 [即，總體法律而非部門規則，一套資料保護原則和義務的核心，賦予個人控制其資料之執行權（例如，資料修正和刪除），以及建立一個具有執行權力的獨立監督機構]。此外，諸如第 108+ 號公約（唯一具有法律約束力的多邊資料保護規章）、經濟合作暨發展組織的隱私準則等國際標準都指出了這方面的積極趨勢。聯合國也正在制定建議之立法規定及現存資料保護規則良好實作彙編，以促進國際間的反恐合作（" 聯合國反恐計畫資料保護 "）。

62. 但正如 2017 年防制洗錢金融行動工作組織《私部門資訊分享指引》所指出的，金融機構依靠當事人同意或公共利益之豁免來處理客戶資料以打擊金融犯罪，包括將資料傳送他人，可能很具挑戰性或根本做不到。此外，必須滿足國際傳輸之合法條件。明確的法律條款規定了適當的保障措施或指引，定義在可能情況下可以為此類目的跨司法管轄區傳輸客戶資料，有助於促進資訊分享。（FATF, 2017[8]）

63. 然而即使有有效的法律架構授權私部門資料的傳送，金融機構分享的資料也可能不準確或不完整。因此，儘管資料合併和協作分析可以幫助其他金融機構遵守防制洗錢／打擊資恐的規定（例如，執行客戶盡職調查），利用這些資訊的金融機構仍有責任確保其準確性。因此，金融機構應透過評估其他金融機構收集檢查之資料是否是最新、適當的且足以履行其防制洗錢義務檢驗證分享資料之品質。

64. 在某些司法管轄區，作為資料控制者的金融機構，（應要求）應向個人提供其所收集、傳輸和保留的資訊的存取權[15]。其目的是讓個人瞭解金融機構擁有關於他們的哪些資料，以便他們可以要求金融機構修正或刪除不正確和不必要的資訊（即在特定條件下修正或刪除不正確和不必要資料之權利）。當涉嫌從事非法活動或正在接受正式調查的個人要求刪除可能讓他被定罪之資訊時，就可能造成彼此之緊張關係。然而，當個人權利的行使可能會影響對法律義務的遵守或正在進行的調查可能受到威脅時，立法可能會規定某些（並有正當理由的）限制。

65. 對於那些允許傳送匿名個人資料的司法管轄區來說，存在另一個挑戰。一些問卷的受訪者指出，在組織分享匿名資料的能力方面存在模糊空間，因為人們認為對匿名[16]和假名[17]的要求並不明確，亦或是在不同的司法管轄區可能有所不同。

66. 此外，關於國際傳輸的規則可能會影響（在金融集團以外）私對私的資料分享。在許多情況下，如果在目標司法管轄區沒有同等或適當的保護或保障措施來確保資料被保護，公共機構或私營機構無法傳輸資料至境外。此外，資料當地化法律通常可能涉及兩個主要要求。（1）個人資料被託管在位於單一國家或多個國家的資料中心；（2）資料在同一國家內被控制和處理。這也對根據各

15 案例詳自動化處理個人資料保護公約第 9 條。

16 匿名資料描述無關於可識別的自然人資訊，或當事人無法再識別的資訊（同時沒有可能重新識別）。（ICO，什麼是個人資料？ 2020 年 12 月閱覽，<ico.org.uk>。）

17 假名資料是一種可取代或刪除資料庫中可識別個人資訊之安全措施。然而，這些資料仍然被認為是個人資料，因為當事人可以被重新識別（例如，如果有人持有加密金鑰）（同上）。

司法管轄區之法律架構的資訊傳輸規定有所限制。因此，金融機構可能被禁止在懷疑有金融犯罪風險的情況下與對造金融機構跨國分享具體資料，同一金融集團亦同，也可能無法像在國內那樣免於承擔責任[18]。

67. 問卷的受訪者最後指出，更廣泛地應用資料庫和協作分析新技術的一個障礙是國內和國際間防制洗錢／打擊資恐與資料保護及隱私權主管機關之間缺乏互動。這種缺乏協調與合作的情況可能會不符合防制洗錢金融行動工作組織第 2 項建議的要求，即相關防制洗錢／打擊資恐當局之間應開展合作並酌情進行協調，以確保防制洗錢／打擊資恐要求與資料保護及隱私權規則的兼容性。

6.2. 資料品質

68. 各個機構、司法管轄區、基礎設施和資訊網路的資料標準和格式差異很大，這些差異可能會阻礙資料分析之利用、拖延銀行程序並增加合規成本。低品質的資料、包括不準確或過時的資料，也可能使資料庫和協作分析的好處化為烏有，因為它可能導致錯誤的分析結果。自動化和先進的分析工具，尤其依賴於標準化的輸入。

69. 根據調查問卷的結果，資料品質是在中心化或分散式的資料庫中部署進階分析的一個主要挑戰。受訪者特別指出，一些金融機構的資料品質很差，而且各金融機構的資料標準存在差異和不相容。為防止產出有偏見的結論，資料品質仍然是以正確和一致的格式產生所需資料庫的主要障礙，在最壞的情況下，這可能導致金融

[18] 更多資訊詳（IIF，2019[17]）。

之排斥性。當資料被加密層覆蓋時又會使這些問題被放大，因為這使得識別資料中的錯誤更加困難，而這又會導致更多的錯誤被輸出。

6.3. 缺乏明確之監管

70. 相當多的問卷調查受訪者指出，缺乏對使用新技術的明確監管要求和指引是對私部門匯集資料及使用協作分析的挑戰。一些司法管轄區正在試圖闡明或調整其規則，以允許金融機構之間的資料分享和協作分析，少數司法管轄區還建立了金融情報分享夥伴關係。部分受訪者指出，在缺乏監理機關的指導和確定性的情況下，優先投資和實施可促進協作分析的昂貴新技術的動力比較小。
71. 還有一位受訪者指出，目前的法律架構建立時沒有考慮到使用新的強化隱私技術的可能性，因此沒有明確說明應用這種技術的分界線。
72. 最後，一些受訪者還指出，現有的國家法規完全禁止私對私的資料分享（除非資訊交流發生在金融集團內部）。

6.4. 可解釋性與可理解性

73. 2020 年 1 月歐洲銀行監理機關（EBA）發佈了一份關於歐洲銀行系統使用大數據和先進分析的文件。這份文件指出，歐洲金融機構似乎處於使用先進分析的早期階段，這些分析使用簡單的機器學習模型，並優先考慮可解釋性及可理解性。採用更複雜的分析模型相關的挑戰之一是其對監管者的可解釋性及可理解性，以及可能出現的偏見和意外結果。根據歐洲銀行監理機關，當一個模型的內部行為可以被人類直接理解（可理解性），或者可以為導

致其輸出結果的主要因素提供解釋（理由）時，該模型就是可解釋的。（EBA, 2020[11]）在缺乏這種理解的情況下，該技術會被監管者視為一個 " 黑盒子 "。這可能會影響其應用，因為監理機關無法進行充分檢查、風險評估，以及無法適當地管理和減輕與使用這種技術有關的任何已確定之風險。特別是當決策是基於高度自動化並對客戶有直接影響時更是如此。為應對這些挑戰，監理機關可與公部門和私部門的技術專家及其他利益相關方合作，評估並幫助推動採用適當的做法，以解釋、記錄和管理防制洗錢／打擊資恐應用中的進階分析技術[19]。這項工作可包括是否以及如何根據風險基礎法適用可解釋性之要求，例如當模型對業務連續性的潛在影響和／或對客戶的潛在危害增加時施加更嚴格之可解釋要求。

74. 一些問卷調查的受訪者指出，金融機構在採用新的防制洗錢／打擊資恐技術進行資料分享和分析時遇到了阻礙，因為監理機關希望密碼學和機器學習模型能夠被明確理解。對於那些缺乏對進階密碼學和分析學有足夠技術知識的人力資源的金融機構來說，如果該技術是由第三方供應商開發的，而該供應商對所用技術所依據的技術規格擁有專利權，這尤其具有挑戰性。一位受訪者還指出從監管者來看，演算法模型的設計應允許在相同的輸入資料下可以重現結果，但機器學習並不一定能做到這一點。

---

19 美國聯邦銀行機構關於金融機構使用人工智慧，包括機器學習的資訊和評論要求，詳 www.federalregister.gov/documents/2021/03/31/2021-06607/request-for-information- and-comment-onfinancial-institutions-use-of-artificial-intelligence。另請參閱金融監管實驗室和史丹佛大學在美國聯邦銀行機構要求提供資訊後提出的類似倡議，該倡議旨在評估解釋、記錄和管理用於貸款承銷的機器學習模型的新興做法：https：//finreglab.org/ai-machine- learning/explainability-and-fairness-machine-learning-in-credit-underwriting/

75. 問卷調查者提出的一個重要因素是，審查進階分析（如人工智慧和機器學習）的結果需要人工（人類）介入，以為確保結果的準確性並持續完善演算法模型。受訪者指出，當人類從執行簡單模型可以完成的基本這種混合方法是一種良好的做法。然而受訪者同樣也擔心，金融機構在沒有深入瞭解技術的功能和目標的情況下使用一些進階的分析方法，可能會導致未經核實和不可靠的輸出。同樣地防制洗錢／打擊資恐的監管人員也應瞭解或有機會接觸到能夠瞭解進階分析模型的團隊，以測試金融機構如何設計和驗證其模型。

76. 最後，受訪者留意到受監管的機構不僅可以向其監管者確認，更要向自己確認，正在應用的任何新技術比以前的系統產生了更好的結果，特別是在可能不清楚該技術是否提高防制洗錢／打擊資恐的效率，這一點很重要。

6.5. 可疑交易報告之保密與洩密

77. 可疑交易報告的保密規則可能妨礙分享可疑交易報告（或已提交可疑交易報告這件事或可疑交易報告中基本資訊）的能力。可疑交易報告的保密性對於申報制度是否有效運作至關重要。STR 的機密性是必不可少的，這樣可疑交易報告的主體和第三方就不會被洩露，因為這可能對情報收集和調查產生不利影響，並可能使當事人潛逃或處置資產。同時保密性還能保護可疑交易報告被申報的當事人聲譽。最後，保密性提供了申報人之安全和保護，違反保密性有可能破壞整個可疑交易報告制度。在許多司法管轄區，未經授權披露可疑交易報告還可能導致金融機構面臨刑事責任。這些問題對可疑交易報告的分享進行了必要的限制。（FATF, 2017[8]）

78. 在跨國分享可疑交易報告時，因為牽涉不同的國家法律，其保密性就更加複雜。例如，可能包括在司法程序中可取得紀錄之可開示性和提供之國家規定。雖然一些國家的法規要求監理機關通知有關國內可疑交易報告的司法請求和傳票，以便監理機關能夠進行介入並確保可疑交易報告在法律程序中的保密性，但這些法規可能無法對提交給外國金融情報機構的外國可疑交易報告提供保護。

79. 然可疑交易報告的保密性會給私對私間的資訊分享帶來挑戰，但防止洩密至關重要。保證個人資料匿名化或加密的替代性法律或技術機制可能能夠提供保障，而無須對防制洗錢／打擊資恐的有效性產生相應的成本。

6.6. 市場結構與競爭

80. 廣泛收集和分析資料並不是件新鮮事，但技術革新使人們有能力儲存大量的資料並馬上對其進行分析，而且資訊量越大分析結果就越有可能準確。目前只有大型且負有職責的金融機構擁有足夠龐大的資料庫來有效使用進階資料分析。因此，我們有必要提高對跨機構資料處理的認識，以確保中小型金融機構也可以從這些新技術中受益，確保與使用這種技術有關的成本優勢可以被這些機構所利用。

81. 不少問卷調查受訪者所指出的，處理大量客戶資訊的金融機構之間有可能互相競爭。這可能導致金融機構僅與少部分＂受信任＂參與者選擇性分享資料，從而形成不平衡的分享架構。如此一來，可能會出現洗錢／資恐的風險從擁有資訊分享機制的金融機構轉移到缺乏此類機制之金融機構，被前者阻撓的犯罪分子為了減少

被發現的可能而被後者吸引。因此，缺乏資訊分享機制的金融機構或部門可能面臨額外的洗錢／資恐風險，可能必須考慮額外的降低風險措施。

82. 金融機構也可能不情願分享有可能改變市場競爭現況的敏感商業資訊。金融機構間不同的資訊技術能力也可能阻礙資訊的有效分享，因為不相同或不完善的資訊技術系統或那些各不相容的資料格式，讓資訊無法被彙總在一起並進行分析。而這也可能使那些依賴傳統資訊技術基礎設施和系統的金融機構處於不利地位，從而導致它們被排除在資料分享計畫之外。

83. 金融服務公司的競爭力越來越受到即時大數據資料庫之存取的影響，所以更不應該讓少數的金融機構因為能存取、交換資料而讓它們獲得不公平的優勢。因此，反壟斷的競爭法可能在評估防制洗錢／打擊資恐的資訊分享工作籌畫時特別重要，即確保維持一個公平的競爭環境，避免潛在競爭者的排他行為。因此，當授權資料使用時，必須以公平、合理和非歧視性的條件，並以不會促成通謀虛偽的方式行之。此外，資料交換必須限制在嚴格必要的範圍內。

6.7. 技術成本與限制

84. 部分的問卷受訪者指出，強化隱私技術和進階分析的可擴展性尤其受到其龐大的啟動成本所影響。大型金融機構可能有資源投資於此類技術或購買授權以存取第三方之技術，但許多小型或中型機構在更新現有傳統技術方面仍然滯後。這也可能導致可得資料庫的減少，因為它可能只包括那些能夠負擔得起與此類技術相關的啟動成本的金融機構之資料。

85. 問卷調查者還指出，機器學習等進階分析方法的應用和維護費用昂貴。由於需要將新的分析方法和舊系統整合，導致額外的升級成本，這就進一步加劇了這種情況。在運行現有系統的同時試用新的進階分析技術所牽涉其中的成本過高也被指出是一個障礙。此外，使用相關進階分析法另一個額外成本是需要維持擁有相關資格技術專長的技術專家，以開發複雜的模型並不斷對其進行完善。

86. 合併和分析大量資料的另一項技術挑戰是需要有足夠的計算能力來運行演算法模型。資料庫的大小會顯著影響計算力的成本。

87. 防制洗錢／打擊資恐資料的合併或分享還可能涉及，像是傳輸包括交易和客戶資訊的大型資料庫。這種大型資料庫很＂重＂（即被稱為資料重力），難以移動。因此，在制定資料彙整計畫時，必須考慮資料重力，以及資料重力一旦集中後的增長潛力。

88. 最後，在防制洗錢／打擊資恐方面部署機器學習等進階分析方法的另一個挑戰是需要驗證資料，或確認個別模式是否真正標明犯罪行為。在洗錢／資恐的脈絡下，驗證模型可能特別困難，因為調查可能需要幾年時間才能結束。在許多情況下，金融機構並不會被告知提交給金融情報機構的可疑交易報告的最終結果，也不知道所申報的活動是否遭致洗錢或資恐定罪。

6.8. 防禦性申報與去風險化

89. 通常所說用於防制洗錢／打擊資恐目的之協作分析是為了查明跨多個金融機構的犯罪行為。通過利用強化隱私技術，一個機構可能能夠克服資料在地化問題及可疑交易報告保密要求，在沒有獲得機敏的基本資料同時獲悉其他機構是否針對自己客戶提交了可

疑交易報告。然而，這有可能會加劇申報可疑交易報告的防禦性行為。過分依賴可疑資訊分享系統有可能導致金融機構僅根據第三方資訊將客戶視為可疑，而這些資訊可能是不準確的，或者懷疑的理由最終被金融情報中心拒絕。這可能會產生意外、不道德的後果，即拒絕合法客戶進入金融系統的影響，或因為要客戶進一步澄清其交易的性質和目的，而導致銀行服務的執行出現延誤。

90. 此外，僅僅只因為懷疑，並不意味著收到資訊的其他機構必須照計畫去提交可疑交易報告。相反，它可能是一個讓機構進行分析風險然後導致強化客戶盡職調查的重要因素。因此，大量引入的協作分析和資料庫可能會導致發現可疑的情況增加（特別是在發生防禦性申報的情況下），並在可能導致合規成本大增的情況下，機構大量實施強化客戶盡職調查。這可能會阻礙對這一技術的使用，或導致去風險化的行為。

6.9. 安全性

91. 引入新技術來彙整及處理資料，帶給網路犯罪分子可以識別並利用安全弱點之新且重大的漏洞和可能性。例如，使用各種技術建立一個集中的資料庫會引起嚴重的網路安全性漏洞，以及國家安全問題，還引起重要的政策顧慮，即誰最終負責監測這些資料存儲的安全，以及誰將對故障或網路攻擊負責。彙集更多的資料也會造成單方發生災難性的大規模資料洩漏的可能性。因此，隨著資料彙整和分享可能性的增加，內部威脅的保護就更加重要。

92. 在協作分析方面使用假名化技術的進步提供了一些保護，前提是識別資訊被分開保存，並受技術和機構措施之約束，以確保個人資料不被歸於一個已識別或可識別的自然人。然而，儘管假名化

技術取得了進展，但資料保護立法仍然適用，並且還應考慮重新識別的風險，根據資料性質、使用背景、可取得之重新識別技術和相關成本，評估所需之時間、耗費之精力和資源，。在涉及使用假名化技術進行協作分析時，資料保護及隱私權主管機關的嚴格監督也是必要的。

6.10. 避免人工智慧分析偏差

93. 一個關於使用資料分析（即人工智慧）來合併資訊時的關鍵考量是，任何先進的分析方法都要排除人的偏見（例如，對宗教、種族、性別、年齡、性取向、種族等之區別對待），從而防止歧視。偏見可能通過引入（或排除）某些資料或在演算法模型的程式設計時被導入系統[20]。這些分析的開發和培訓必須包括無偏見的資料，並開發不會加深人類偏見或歧視的演算法。

6.11. 人權

94. 為了商業考量，私部門的實體可能支持對個人進行分析，而這最終可能導致歧視，例如對種族、性別、政治傾向或宗教信仰的區別對待。因此，監督機構和資料保護及隱私權主管機關需要對任何用於資料庫和協作分析的工具進行充分的通透和嚴格的監控和／或監督。這包括使用假名化技術的工具，因為這些工具有可能重新追蹤，以推斷出資料庫中所包含的個人資料和身份。

---

[20] 關於人工智慧倫理的更多資訊，詳（FSB，2017[15]），附件 B。

7. 廣泛運用資料庫與進階分析

95. 根據問卷，受訪者為促進更多使用新技術進行資料彙整和協作分析，以及應對上述的一些挑戰，最常引用的解決方案是提高這些新技術的監管確定性。下文總結了由受訪者和私部門之利益關係人發現的各種解決方案，這些解決方案有助於更好地利用新技術進行私人間的資料分享和分析。這些解決方案為防制洗錢金融行動工作組織未來可能開展的工作，和其與私部門和資料保護及隱私權主管機關之間的對話提供了一個起點。防制洗錢金融行動工作組織尚未認可這些有助於為更廣泛地使用資料庫和協作分析創造有利環境的因素。

7.1. 監管透明度

96. 問卷受訪者指出，現在越來越迫切需要制定一個納入與私部門間分享或彙整資料相關的資料框架，其中包括防制洗錢／打擊資恐資料。問卷受訪者回覆指出，這可以通過加強防制洗錢／打擊資恐主管機關（包括監理機關）和資料保護及隱私權主管機關之間的合作來實現。這可能有助於營造一個能夠減輕行業因目前監管缺乏明確性而產生的規避風險的有利環境。大部分受訪者還呼籲國內金融監理機關提供明確指引，說明金融機構之間有哪些資訊是可以分享的，以及某些技術（如同態加密等）和流程是否能夠使各機構繼續遵守國內和跨國際的隱私要求，除了以上要求還要能制定專屬於金融產業之法規。這可以為金融機構提供以繼續投資於技術、培訓、人力資源和資料分享解決方案的生產應用所需的保證。一些受訪者也呼籲整合並公佈新技術的有效案例（即最

佳實踐），並詳細說明某些新技術如何解決與私營機構間資料分享有關的隱私問題。

97. 部分受訪者還呼籲制定國家法律安全港條款，俾允許金融機構之間在必要性和相稱性之原則下為防制洗錢／打擊資恐目的自願分享資料。

98. 對於防止可疑交易報告洩密的相關規定，一些受訪者呼籲修改可疑交易報告的監管要求，讓金融機構能夠更自由地分享不論是關於是否針對某個人提出的可疑交易報告，或是報告的相關資料。

7.2. 提升使用環境

99. 一些受訪者還呼籲防制洗錢／打擊資恐的監理機關推出更多的實驗性方案、監管沙盒和創新中心，以便金融機構在沒有懲罰或過於嚴苛的監管執法的情況下開展測試資料分享和分析的新技術。這將促進這領域的創新，蓋金融機構不會因試驗最終證明是不成功的，而受到監管部門的指責。此倡議之成功與否，也因國內資料保護及隱私權主管機關之參與及投入程度而受到影響。這樣的參與可以促進結盟聯合、共同學習，並在遵守資料保護及隱私權要求的情況下，提高對模型治理、建模技術以及資料分析如何針對特定的洗錢／資恐風險領域和促進資料分享等問題的釐清。

100. 防制洗錢金融行動工作組織還確定支持在防制洗錢／打擊資恐方面使用技術的建議行動（見附件 C），以更進一步推動追求積極和負責任的創新的 2017 年聖荷西原則。這些行動指出，用於防制洗錢／打擊資恐的新技術之開發與執行，須反映各種威脅與機會，確保其使用符合資料保護和隱私以及網路安全的國際標準。

7.3. 資料標準化與管理

101. 一些受訪者呼籲，為了提高資料品質，應對資料收集要求用標準化之格式，並促進使用開放的應用程式介面，使客戶能夠在金融機構之間分享資料。然後，各司法管轄區可以利用其合規權力作為回饋機制，向金融機構通報資料品質要求，並採取適當措施以提高品質至可接受的水準。

102. 在資料治理方面，受訪者強調金融機構需要制定資料治理的政策、架構與控制措施，以確保：

    a. 資料的品質，包括資料的完整性，最新資料是如何收集或更新的，資料的結構是否為機器可理解的格式，以及資料的來源是否會影響或依賴對資料的解釋。以上也包括評估資料真實性的方式；以及

    b. 追蹤資料的來源，包括保留資料的審計存底。

103. 利用數位身份來進行識別也是解決資料品質的一個可能的解決方案，因為它可以成為一個用來支持依賴第三方做身份辨識的標準工具，從而有助於增加資料分享。同樣，法人機構識別碼可被用作法人的客戶盡職調查的文件來源。納入法人機構識別碼可以確保每個法人都有一個獨特的識別號，而不是依賴名稱匹配。

104. 最後，在與受訪者的訪談中，共同申報準則（CRS）被引用為模型。共同申報準則為了打擊逃稅行為，要求各司法管轄區從其金融機構獲得具體資訊，並每年與其他司法管轄區自動交換資訊。（OECD, n.d.[12]）這些受訪者認為，這種模式可以為基於防制洗錢／打擊資恐目的而分享資料之品質提供參考，因為它的要求包括具體的資料標準化（即，規定要收集和交換的資訊）。

7.4. 人工智慧偏差預防

105. 最後，為了防止人工智慧的人為偏差和歧視，受訪者強調定期審查資料來源的合法性、可信度、全面的模型驗證，和持續的模型監控的重要性。例如，資料庫可能需要額外資料之訓練，來提高準確性和公平性，以彌平資料庫可能對某些群體的代表性不足或過高。

106. 此外，經濟合作暨發展組織成員國於 2019 年 5 月通過的經濟合作暨發展組織人工智慧準則指出，人工智慧系統應在顧及法治、人權、民主價值和多樣性等原則來設計，並應包括適當的保護措施，例如於必要時能夠進行人工干預以確保社會的公平和公正。人工智慧系統還必須在其生命週期中以穩健、安全的方式運作，同時持續評估和管理潛在風險。因此，必須從一開始就充分理解在監管環境中使用預測模型的道德規範，因為那些開發、應用或操作人工智慧系統的組織和個人可能要對其正常運行負責。（OECD，2019[13]）

8. 結語

107. 在私部門之間的防制洗錢／打擊資恐資料分享所斟酌的因素對防制洗錢金融行動工作組織來說並不新鮮。然而，現有及新興技術的進步可能會提供新的分享和分析資料的方法，以便更有效地發現潛在的可疑活動或遵守其他防制洗錢／打擊資恐的義務。為了更好地保護個人資料，新技術也可能提供解決方案，確保任何資訊的交流或處理都顧及國內和國際間資料保護及隱私權之法律架構。然而，在實施之前，需要對所考慮的發展是否符合司法管轄區的資料保護要求進行適當評估，以免妨礙對基本權利的保護。例如，在一些司法管轄區，這種措施目前可能在法律上是不允許的。

108. 本評估報告盤點了現有或新興的能促進金融機構之間資料庫和協作分析之技術，並研究了受訪者所提出的政策考量、法律挑戰以及潛在解決方案。本報告發覺，在提倡資料庫和協作分析措施也呈現不少重要的政策考量。例如，重要的是資料庫的使用和協作分析應該平等權衡，並減輕與去風險化以及在執行之前有關拒絕合法客戶存取金融系統之任何風險。防制洗錢金融行動工作組織將基於本文件的基礎上，繼續在防制洗錢／打擊資恐的監管者、技術開發商、金融機構和資料保護與隱私權主管機關以及其他相關專家之間開展對話，以確保這些有助於提高防制洗錢／打擊資恐效力的新技術可以得到充分利用，並符合國內和國際間資料保護與隱私權法律架構。

附件 A、詞彙表

進階分析：進階分析是指使用複雜的技術和數位工具，來自主或半自主地檢查資料或內容，通常在超出傳統商業智慧的範圍發掘更深層次的見解，進行預測或給出建議。進階分析技術包括那些諸如資料／文本探勘、機器學習、模式匹配、預測、視覺化、語意分析、情感分析、網路和集群分析、多變數統計、圖形分析、類比、複雜事件處理、神經網絡。進階分析法通常依賴於大數據的使用。

應用程式：應用程式是為幫助使用者執行特定工作而設計的電腦軟體。

應用程式介面（API）：應用程式介面是一套用於構建和整合應用軟體的定義和協定。應用程式介面讓電子產品或服務可以隨時與其他產品和服務進行交流。

演算法：電腦演算法是一組執行特定工作的連續指令。

人工智慧（AI）：人工智慧系統是一組針對人類定義的目標，（並以不同程度的自主性運作）做出會影響真實或虛擬環境的預測、建議或決定的機器系統（OECD, 2020[14]）。人工智慧的目標是使電腦能夠自動進行某些方面的分析，盡可能地節省在枝微末節的工作上耗費的人力，並獲得人類可能無法得出的見解。人工智慧在眾多應用程式中都有幾個部分的技術組成，對於什麼是＂思考＂、什麼是＂智慧＂、什麼是＂完全自主＂，目前並沒有達成共識，而且人工智慧有幾個類別。但總的來說，人工智慧系統在不同程度上結合了意圖性、智慧和適應

性等特性上建立了所謂的 " 智慧型機器 "。目前最為人所知及最發達的人工智慧形式是機器學習。

大數據：金融穩定委員會將大數據定義為 " 由於越來越多地使用數位工具和資訊系統而產生的大量資料 "，像是金融交易、社交媒體和機器（如物聯網、電腦和手機資料 , FSB, 2017[15]）所產出的資料。

黑盒子：黑盒子是指人工智慧／機器學習或其他技術以不透明、非直觀的技術且不提供有關其決策和預測／結果的充分資訊，亦即黑盒子技術缺乏可解釋性。

基準化分析：基準化分析是一種確定以技術為基礎之流程、生產或服務的實際能力和相對能力之方法；透過與功能、工作或目標的最佳性能進行測試，使用由特定基準來衡量之精準資料以確定性能差距，透過無論是在特定的實體或組織內，還是在整個行業內或者由不同的行業實現。基準測試可被用作衡量或比較在新科技和傳統系統之間或是在新科技和相對之替代新科技的效能評估。

協作分析：對於協作分析，資料不會被轉移集中到一個位置，以便與其他資料庫一起分析。相反地，分析工具會反過來移到資料上。這使得保持資料的安全和讓「知道是誰、為了什麼目的、訪問什麼資料」這些事情更加容易被控制。

網路安全：網路安全指的是包含了資料保護以及移動、儲存和驗證資料的系統的所有過程，是一個比資料安全更概括的術語。

資料庫／彙整：資料彙整是指將自不同來源的數據資料被結合起來，形成一個更全面和更有效的資料庫進行分析（包括由多方）一個過程。這些資料庫是以中心化方式組織起來的。

資料安全：資料安全是指在其生命週期內保護其資料免受未經授權的存取和資料惡化的過程。資料安全的做法包括資料加密、雜湊、記號化以及保護所有應用程式和平台的資料的金鑰管理做法。資料安全的定義比網路安全的定義更有侷限性。

資料標準化：資料標準化是為了讓不同使用者能夠處理和分析資料，將資料轉換為統一格式的過程。這種標準化對於實現大數據處理和進階分析，以及其他創新數位工具和方法的開發和應用至關重要。例如，金融資料在實體內部和實體之間都可能有所不同；資料標準化將其轉換為一種通用的形式，從而實現複雜的大規模分析。

數位身份（ID）系統／解決方案：數位身份識別系統或解決方案是一種執行識別或驗證（自然人或法人）身份的識別系統、產品或服務，將已驗明正身的身份與數位憑證結合起來，然後將數位憑證和其他可能的驗證要件來建立（確認）聲稱的人是擁有身份的人（即，他就是他所宣稱的那個人）。

分散式帳本技術（DLT）（亦稱區塊鏈）：分散式帳本技術指的是一種能夠讓數台電腦（通常是位於多個實體或地點）同時存取、驗證和更新分佈於其上的不可更改帳本（電子記錄）的技術協議，意即分散式帳本技術可以創建一個分散式數位資料庫。

深度學習（DL）：深度學習是一種具有多（深度）層的人工神經網絡（受人腦啟發的演算法）以高度自主的方式從大量的資料中學習的進階機器學習技術。深度學習演算法反復執行同一項工作，每次都會稍作調整以改善結果，使機器能夠在沒有人類介入的情況下解決複雜問題。

數位化技術：此項技術是利用數位化技術和數位化資料來改變商業模式，對於工作的完成方式產生影響，改變客戶和公司的互動方式，並提供新的收入和創造價值的機會。

資訊數位化：數位化是將資料、資訊、文字、圖片、聲音或其他類似的表現形式轉換為可由電腦處理的數位形式（即二進位碼）。
*動態資料：*動態資料指的是連續且資料點不停變動的即時數位資料，因此資料庫隨著時間的推移不斷變化，這與靜態或持續而不受時間影響的資料不同。

可解釋性：在使用新技術的背景下，可解釋性是指基於技術的過程、解決方案或系統可被解釋（分析）、理解和說明。可解釋性提供了對解決方案如何運作和其產生之結果的充分理解，是可信的和負責任的使用的基本條件。可解釋的人工智慧技術提供了用於實現結果的資料、變數和決策點的透明度。

金融科技：金融科技泛指在金融領域為了各種不同的目的使用之新興數位技術。一開始金融科技主要是指利用基於技術的創新來提供諸如移動支付解決方案、線上借貸服務、演算法儲蓄和投資工具、虛擬貨

幣支付、募資（眾籌）和接受存款（遠端存款服務、行動銀行）等面向客戶的全新金融產品和服務。金融科技現在還包括使用新興技術提供如使用演算法、大數據、人工智慧和機器學習，以及用於收購清算、結算和其他收購仲介公司的連結分析，例如證券、衍生品、零售金融和支付，以及監管合規活動（見下文監管科技定義）等的自動化中、企業後臺功能。其他應用仍有待開發

模糊邏輯：模糊邏輯是人工智慧的一個子集合，它接受一個開放的、範圍不精確的資料（不精確的輸入），以一種產生的輸出包括在是與否（例如，肯定是、可能是、不確定、可能不是、肯定不是）之間的一系列居中可能性的方式處理多個值。模糊邏輯系統對不完整的、模糊的、扭曲的或不準確的（模糊的）輸入產生明確的輸出，比傳統的是／否邏輯更接近人類的決策。模糊邏輯可以通過硬體、軟體或兩者的結合來實現。

物聯網（IoT）：由所有支援網際網路的設備和機器組成之全球網路，這些設備和機器與網際網路相連，在沒有和人互動的情況下利用嵌入式感測器、處理器和通訊硬體在收集、發送、分享資料同時採取行動。物聯網產生了大量的即時資料，這些資料可以被分析並用來創造預期行動或商業成果（見大數據）。

可交互運作性：是指不同的資訊技術系統和應用程式軟體間，能夠實時地溝通、交換資料和不間斷使用資訊的能力，使所有參與者在所有系統中操作。

機器學習：機器學習其中一種人工智慧類型（子集合）是用來 " 訓練 " 電腦系統，它能夠從資料、識別模式來學習，並在最小的人為介入下做出決定。機器學習涉及到透過經驗和不斷發展的模式識別演算法設計一連串的行動，在有限的或沒有人類干預的情況下自動解決一個問題；也就是說，它是一種可以自動建立分析模型的資料分析方法。

機器可讀規則：機器可讀規則用電腦程式取代了用自然法律語言編寫的規則，以便能夠使用人工智慧進行監管申報。

自然語言處理（NLP）：自然語言處理是人工智慧的一個分支，使電腦能夠理解、解釋與操縱人類語言。自然語言處理使人類可以與機器對話。

強化隱私技術：" 專業的加密能力，允許在底層資料上進行計算，而資料所有者不一定會洩露該底層資料。同樣的技術可以確保資料所有者對搜索查詢沒有可見性，查詢和結果仍然是加密的（或不披露），只有請求者得知 "。（Maxwell, 2020[16]）因此，這個術語包含了一系列使用加密的技術，主要在資料使用過程中允許保護隱私。

即時分析：即時分析是一個系統處理和分析實時載入的資料，並幾乎馬上（接近即時）產生有意義（例如，資訊、預測或決策）輸出的機器學習過程。

即時資料（RTD）：即時資料是在收集後立即傳送的資訊，確保所提供資訊的及時性。即時資料能夠實現即時分析，可以是動態的、也可以是靜態的（例如，一個在特定時間、特定位置即時寫入的資料）。

監管科技（RegTech）：監管科技利用比現有技術更有效的新技術來遵守監管要求，是金融科技的一個子集合。

*負責任創新：*當創新技術在防制洗錢／打擊資恐、消費者保護、網路安全和隱私保護等面相能勝任其目的並符合適用的監管要求，就是負責任的創新。

智慧機器：智慧機器是使用人工智慧演算法的電腦硬體和軟體系統，被設計使用即時資料來做決定。與只能做出機械或事先安排的被動機器不同，智慧型機器使用結合來自感測器、數位資料和遠端輸入，即時分析這些不同來源的資訊，並根據從中得出的見解採取行動。智慧型機器透過使用進階的計算過程模仿人類智慧，根據計算結果即時分析得出結論。

靜態資料：靜態資料指的是一個固定的，資料在被收集後保持不變的資料庫。

監督式學習：監督式學習是一種透過向演算法提供已知結果的輸入資料來指導演算法預測模型的機器學習過程，即利用實例以來教授演算法。輸入／輸出對（標記的資料）為演算法提供回饋，演算法使用訓練資料庫來調整模型以最小化誤差。例如，一個訓練集可能包含不同種類已經被標籤的動物圖片，允許演算法將預測的標籤與正確的標籤進行比對。監督式學習使用驗證資料庫，來衡量演算法在學習模型方面的進展，並使用測試資料庫來評估模型在還未見過資料上的表現，以確定模型是否有效地學習了訓練資料，並能歸納到新資訊。

監理科技（SupTech）：監理科技是指監理機關用於支援監督和審查之新技術。

非監督式學習（亦稱非監督式機器學習）：非監督式學習是使演算法能夠在無人工介入下，分析和協同未標記的資料庫以發現隱藏的模式、資料分組或異常情況的一個機器學習過程。該演算法對可用資料進行分析，並在沒有解答的情況下，透過推論和基於開放觀察和直覺，對同類事物進行分組，來確定相關性和關係。它的建模會隨著演算法接觸的資料量增加而變得更加準確和完善。

附件 B. 關於私對私防制洗錢及打擊資恐資料分享與分析新技術之其他監管科技案例研究

案例研究：使用同態加密的加密搜索試驗計畫

監管科技公司與一家金融機構合作，實施強化隱私的銀行內資訊分享系統。該技術使用同態加密，允許金融機構對金融犯罪和合規進行加密查詢，同時確保監管合規。目前監管科技公司與金融機構正在努力將更多的銀行加入該計畫，還有正在定義包括同銀行的跨境客戶風險評級和閾值模型的新案例，並進一步應用在產品上。同態加密被特意應用於該計畫，以保護敏感資訊不被暴露，但成員仍能夠使用資料進行分析和在機構間比對。保護隱私的分析能力的優勢在於，它可以發出搜索查詢的結果而不會對其他機構揭露查詢關鍵詞。這會讓披露、洩密和違反法規的風險被抵銷，同時為潛在的參與機構提供了分析能力。這個專案的主要障礙是在什麼類型的資料可以分享、在什麼情況下分享，以及如何分享方面缺乏監管明確性。

案例研究：德國合作分析平台

金融科技公司正與一個由大型銀行、軟體供應商和學者組成的聯盟合作開發一個以打擊金融犯罪的新合作分析平台。該平台將跟機構間的交易資訊分享和金融資訊的資料庫和分析工具組有關。因為這個平台體現在整個金融系統，而非個人金融服務提供商之中中，它將對所有金融機構就犯罪行為和犯罪網路提供全新見解。有了這些情報，德國和歐洲的金融機構將能夠在更廣泛的金融系統中構建一個關於其客戶整體活動網路的新視角，從而通過暴露以前被掩蓋的交易行為的隱蔽關係和模式，讓防制洗錢的大網更細緻。

案例研究：北歐實名認證平台

北歐國家中最重要的六家銀行於 2019 年成立一家監管科技公司，目的是為了解決北歐市場防制洗錢法規方面的挑戰提出一項聯合倡議。這六家創始銀行為實名認證資訊制定了一個共同的資料標準，透過該公司在終端客戶／入口網站提供實名認證服務和數位平台。該公司的平台是完全獨立的，參與的金融機構如果需要有效和合規的實名認證資訊都可以使用。這確保了金融機構可以登入並使用這些實名認證資訊作為他們自己的風險評估的基礎。因為建立金融關係變得更容易，客戶體驗更加友好，這也對他們的客戶更有利。對客戶關係的控制權仍在金融機構手中。公司透過使用基於隱私和安全設計原則的安全混合雲端服務架構，確保整個解決方案的個人資料隱私受到保護。

案例研究：金融犯罪指數

銀行 A 開始使用監管科技企業的金融犯罪指數來加強他們對金融犯罪風險的處理。該指數利用銀行自身的資料，結合公開資料和監管科技企業的專有資料庫，每月生成整體金融犯罪風險分數，以及九個金融犯罪風險主題的分數和報告。

案例研究：安全的端到端加密平台

一家監管科技公司建立了一個使銀行和其他金融機構能夠交換與防制洗錢有關訊息的訊息及資訊交換平台。透過該平台交換的資訊可用於一對一的資訊傳遞（資訊請求）或一對多的 " 資料庫 "，可以幫助金融機構：（1）解決更根本的查詢（像是需要對照金融機構對制裁警示提供額外資訊）。（2） 更複雜的聯合調查（像是調查涉及多個機構的次級交易監控警報），以及（3） 讓高風險客戶的盡職調查資料更充

實（例如，分享有關重要政治性職務之人、其家庭成員及有密切關係之人、實質受益人、資金來源等資訊）。

該平台由端對端加密技術建立，所有交換的資料都受到加密金鑰和密碼來保護。單邊加密和雜湊法被用於資料庫，因此金融機構可以與多方分享資訊，並通過雜湊法驗證所交換的資料或文件的真實性。平台主機不能使用任何未加密的資料，平台透過記錄所有關鍵活動來確保絕對的可審計性。

案例研究：使用同態加密進行記錄的盲匹配

一軟體公司與國家機構合作進行試驗計畫，利用同態加密技術實現記錄的盲匹配。該國家機構希望從一系列私部門和公部門（包括多個金融機構）收集和聯結資料，用於統計目的，為公共政策提供資訊。解決方案提供商結合使用技術和結構控制，允許資料貢獻者向接收者提交加密資料：

1. 只有加密的資料能脫離貢獻者的環境。
2. 資料在到達接收方之前不能被聯結。接收方需要一個第三方參與者（中間人）將加密的貢獻者資料轉換為可連結的、記號化的資料庫。
3. 接收方無法逆向處理並獲得原始的貢獻者資料，只能夠連接資料庫。

試驗計畫成功地證明，該解決方案能夠在一個在離開接收方環境後，對任何一方都是可見共同屬性上，實現聯結資料的運作。這允許進行人口分析的同時也能保護個人的隱私，為政策制定提供資訊。該技術目前已由英國健保署電腦部門投入使用。

附件 C. 關於支持運用科技執行防制洗錢及打擊資恐之行動建議

負責任地使用包括數位身份和先進的交易監控和分析解決方案（包括協作分析）之新技術，可以幫助公部門和私部門能有效地、依風險基礎法實施防制洗錢金融行動工作組織的建議，同時促進金融包容性。

以下原則推進 FATF 在 2017 年支持的聖荷西原則*追求積極和負責任的創新*。防制洗錢／打擊資恐的新技術其開發和使用必須不僅反映威脅還要能帶來機會，確保其使用符合資料保護和隱私以及網路安全的國際標準。

1. 政府和私部門為提高防制洗錢／打擊資恐的有效性一起創造有利的創新環境。
    i. 促進應用防制洗錢／打擊資恐措施的創新解決方案並加強對其監督和檢查，包括風險評估、客戶盡職調查和其他要求。
    ii. 更新內部原有舊系統或用新技術取代這些系統的最佳實務做法。
    iii. 新防制洗錢／打擊資恐解決方案的適當保障措施和特點，包括：流程和結果的可解釋性和透明度、人工監督、尊重隱私和資料保護、強大的網路安全、以及與全球、國家和技術標準保持一致的最佳做法。
2. 在應用新技術時確保隱私和資料保護。
    i. 確保在部署新技術處理個人資料時具有有效法律依據。
    ii. 根據國家和國際法律架構保護個人資訊。
    iii. 根據明確、具體和合法的目的處理資料，同時遵守國內和國際間規則。

iv. 支持負責任地開發和採用保護隱私的創新技術，以便在保護隱私的同時，實現強大的防制洗錢／打擊資恐的資訊分享和分析。

3. 設計支持金融包容性促進防制洗錢／打擊資恐的創新。
   i. 通過制定和應用減輕金融包容性障礙的創新解決方案。
   ii. 確保負責任的創新與防制洗錢金融行動工作組織促進金融包容性之目標相一致。
4. 制定和宣傳靈活的、技術中立的、基於結果的、符合風險基礎法的創新政策和監管方法
   i. 在伴隨著結構和組織變化的背景下，全面考慮新技術的影響，其可能產生的意外後果，以及其對防制洗錢／打擊資恐的有效性和金融包容性的總體影響。
   ii. 必要時發佈和／或更新明確的政策聲明、指引、使用案例、最佳做法或法律規定，以告知和鼓勵負責任地使用新技術來進行防制洗錢／打擊資恐的工作。
   iii. 為相關政策和決策過程提供資訊與對照方和受監管法人徵求意見。
5. 實行知情監管
   i. 為了能夠對其使用進行知情的監管和監督建立新技術方面的專業知識，包括為具體的防制洗錢／打擊資恐的目的。
   ii. 在防制洗錢／打擊資恐的監督和檢查中確定明確的、定義清晰的新技術用途。
   iii. 瞭解與新技術相關的風險和利益，以及保持其利益的適當風險緩解措施。
   iv. 使用技術來加強防制洗錢／打擊資恐的監管。

6. 推動和促進合作

   i. 與所有有關當局合作和協調，以促進採取全面、協調的方法，包括資料保護和隱私權主管機關去瞭解和處理在防制洗錢／打擊資恐方面使用新技術的風險和益處。

   ii. 或可考慮發展合作環境，以促進跨政府和／或公、私部門對新技術和創新解決方案的研究和開發。

   iii. 國際間共同制定關於使用新技術進行防制洗錢／打擊資恐的原則，以幫助確保其符合人權、改善國際相關技術標準和信任體系對防制洗錢／打擊資恐的實施、網路安全、資料隱私和保護措施。

參考文獻

歐洲銀行業管理局（2020）, *大數據與進階分析*. [13]

歐洲個人資料保護委員會 （2020,）, *關於保護個人資料與防止洗錢和恐怖主義融資有關的聲明*, https：//edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_20201215_aml_actionplan_ en.pdf. [1]

防制洗錢金融行動工作組織 （2017）, *私部門的資訊分享指引*, https：//www.fatf- gafi.org/publications/fatfgeneral/documents/guidance-information-sharing.html. [10]

金融犯罪執法局 （2020）, *314 節（b）內容概要說明書*, http：//www.fincen.gov/sites/default/files/shared/314bfactsheet.pdf. [11]

金融穩定委員會（2020）, *主管機關和受監管金融機構對監管技術的使用*, p. 32, http：//www.fsb.org/2020/10/the-use-of-supervisory-and-regulatory- technology-by-authorities-and-regulated-institutions-market-developments-and-financial- stability-implications/. [9]

金融穩定委員會（2017）, *金融服務中的人工智慧與機器學習*, https：//www.fsb.org/wp-content/uploads/P011117.pdf. [17]

全球法人識別碼基金會 （n.d.）, *法人識別碼的介紹（LEI）*, http：//www.gleif.org/en/. [21]

國際金融協會 （2019）, *資料跨境傳遞 - 突破資料在地化之障礙*, http：//www.iif.com/Portals/0/Files/32370132_iif_data_flows_across_borders_march2019.pdf [19]

Maxwell, N.（2020）, *創新與討論文獻：利用隱私保護分析應對金融犯罪之案例研究*, http：//www.future- fis.com/uploads/3/7/9/4/3794525/ffis_innovation_and_discussion_paper_-_case_studies_of_the_use_of_privacy_preserving_analysis_-_v.1.3.pdf. [18]

邁克菲（2020）, *什麼是雲端運算安全？*,http：//www.mcafee.com/enterprise/en-us/security- awareness/cloud.html. [7]

微軟（2016）, *同態加密*, http：//www.microsoft.com/en- us/research/project/homomorphic-encryption. [2]

微軟 Azure（n.d.）, *機密運算*, https：//azure.microsoft.com/en- us/solutions/confidential-compute.（accessed on December 2020）. [6]

經濟合作暨發展組織（2020）, *人工智慧原則*, https：//www.oecd.ai/ai-principles. [16]

經濟合作暨發展組織（2019）, *人工智慧原則*, http：//www.oecd.org/going- digital/ai/principles/. [15]

經濟合作暨發展組織（n.d.）, *區塊鍊入門*, http：//www.oecd.org/finance/OECD-Blockchain-Primer.pdf（accessed on December 2020）. [8]

經濟合作暨發展組織（n.d.）, *什麼是共同申報準則？*, http：//www.oecd.org/tax/automatic-exchange/common- reporting-standard/（accessed on December 2020）. [14]

賽仕軟體（2020）, *自然語言處理*, http：//www.sas.com/en_us/insights/analytics/what- is-natural-language-processing-nlp.html. [5]

Scheibner, J.（2020）, *多場域的健康數據研究之資料保護和倫理要求：立法治理架構和資料保護技術作用的比較研究*, http：//www.ncbi.nlm.nih.gov/pmc/articles/PMC7381977/pdf/lsaa010.pdf. [3]

Shiffman, G.（2020）, *“革命性技術的聯盟式學習（白皮書）”*. [4]

Tim Hulsen, T.（2020）, *分享即是關懷—醫療保健計畫中的資料分享*, http：//www.mdpi.com/1660-4601/17/9/3046/pdf. [20]

聯合國貿易暨發展會議（2020）, *國際間資料保護與隱私權立法*, https：//unctad.org/page/data-protection-and-privacy-legislation-worldwide. [12]